

# **EXHIBIT B**

Lesley E. Weaver (SBN 191305)  
BLEICHMAR FONTI & AULD LLP  
555 12th Street, Suite 1600  
Oakland, CA 94607  
Tel.: (415) 445-4003  
Fax: (415) 445-4020  
lweaver@bfalaw.com

Derek W. Loeser (admitted *pro hac vice*)  
KELLER ROHRBACK L.L.P.  
1201 Third Avenue, Suite 3200  
Seattle, WA 98101  
Tel.: (206) 623-1900  
Fax: (206) 623-3384  
dloeser@kellerrohrback.com

*Plaintiffs' Co-Lead Counsel*

*Additional counsel listed on signature page*

**UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF CALIFORNIA**

IN RE: FACEBOOK, INC. CONSUMER  
PRIVACY USER PROFILE LITIGATION

MDL No. 2843  
Case No. 18-md-02843-VC

This document relates to:

ALL ACTIONS

**CORRECTED CONSOLIDATED  
COMPLAINT**

Judge: Hon. Vince Chhabria

## TABLE OF CONTENTS

I.	INTRODUCTION -----	1
II.	JURISDICTION, VENUE, AND CHOICE OF LAW -----	5
III.	PARTIES-----	6
A.	Plaintiffs-----	6
B.	Defendants and Co-Conspirators-----	37
1.	Prioritized Defendant and Doe Defendants: -----	37
2.	Non-Prioritized Defendants (Individual Defendants Named in Actions Consolidated in this MDL As to Whom Co-Lead Counsel Seek a Stay) -----	38
C.	Unnamed Co-Conspirators: Cambridge-Analytica-Related Entities -----	39
D.	Other Non-Defendant Co-Conspirator -----	42
IV.	FACTUAL BACKGROUND -----	42
A.	Facebook’s Transition from Social Media Company to Data Broker -----	42
B.	Facebook Enables Apps, Websites, and Devices to Access Facebook Users’ Content and Information -----	44
1.	How Facebook Enabled Third Parties to Gather and Disseminate Users’ Content and Information -----	44
2.	Cambridge Analytica Used Facebook’s API to Take Users’ Content and Information Without Their Knowledge Or Consent -----	49
3.	The Cambridge Analytica Scandal Has Triggered Seriatim Revelations by Facebook of Third Party Abuse of User Content and Information -----	61
4.	Facebook Also Enabled Device Makers and Other Business Partners to Access Users’ Content And Information Through Friends-----	64
5.	Facebook Disregarded Friends’ Privacy Settings When Transferring Data to Third Parties Through Graph API v. 1.0 -----	66

C.	Facebook Made It Unreasonably Confusing and Burdensome for Users to Prevent the Sharing of Their Content and Information with Third-party Applications. -----	67
1.	Facebook’s “Privacy Settings” Misled Users About How to Control the Information and Content That They Shared with Applications. -----	68
2.	To Control Sharing with Applications, Facebook Required Users to Hunt for, Find, and Change the Default Preferences of Their App Settings -----	73
3.	Facebook Maintained the “Apps Others Use” Control Panel Until April 2018, Following the Cambridge Analytica Scandal -----	77
D.	In the Documents That Purport to Govern the Relationship Between Facebook and Its Users, Facebook Made Promises About Privacy That It Broke, and Also Failed to Properly Disclose the Access to Users’ Content and Information That It Gave to Third Parties. -----	79
1.	What the Statement of Rights and Responsibilities Promised -----	80
a.	The Statement of Rights and Responsibilities Promised to Respect Users’ Privacy -----	81
b.	The Statement of Rights and Responsibilities Promised Users Throughout the Class Period That Facebook Would Not Share Content or Information With Advertisers Without Their Consent -----	84
c.	The Statement of Rights and Responsibilities Promised to Adequately Notify Users When It Was Amended -----	86
2.	The Statement of Rights and Responsibilities Did Not Incorporate or Make Binding Facebook’s Other Policies -----	89
3.	Facebook’s “Policies” Were Generally Difficult to Access, Confusing, and Constantly Changing Without Notice. -----	91
a.	To Access the Contents of the Privacy, the Data Use, and Data Policies, Users Were Forced to Navigate a Maze of Hyperlinks -----	91

b.	Users Often Were Not Required to Read the Contents of the Privacy, the Data Use, or Data Policies When They Signed Up -----	97
c.	The Privacy, Data Use, and Data Policies Made It Difficult for Users to Understand How Facebook Made Their Content and Information Accessible to Third Parties -----	102
d.	The Documents Were Constantly Changing-----	109
e.	Facebook Failed to Adequately Notify Users of Changes to the Privacy Policy, Data Policy, and Data Use Policy -----	112
E.	The Cambridge Analytica Scandal and Subsequent Revelations of Facebook’s Agreements with Third Parties to Share User Content and Information with Third Parties Without Full Disclosure Show that Facebook Violated the 2012 Federal Trade Commission Consent Decree-----	113
F.	Even Prior to the Cambridge Analytica Scandal, Numerous Investigations Questioned Facebook’s Practices With Regard to User Privacy -----	116
G.	Despite Warnings, Facebook Failed to Take Reasonable Measures to Ensure That Third-Party Applications and Device Makers Would Not Access and Use Its Users’ Content and Information Without Their Consent. -----	117
1.	Facebook Partnered With Kogan to Exploit Facebook User Data for Commercial Use -----	118
2.	Facebook Has Repeatedly Ignored Its Users’ Privacy Rights and Expectations-----	118
3.	Facebook’s Failure to Implement Reasonable Security Measures -----	122
4.	Facebook’s Failure to Notify Plaintiffs and Class Members of the Misuse of Their Data Made Remedial Measures Impossible-----	125
5.	The Cambridge Analytica Scandal Has Triggered Additional Revelations About Misuse of User Data-----	125
H.	Statements by Facebook’s CEO Give Rise to a Duty to Disclose and Admit to Injury From Lack of Disclosure -----	126

I.	Facebook’s Cultivation and Release of Its Users’ Data Were Part of a Lucrative Market for Big Data Where Users’ Content and Information is Valuable, Marketable Property -----	131
1.	Facebook Has Generated Significant Revenue from Allowing Access to Its Users’ Content and Information-----	131
2.	Facebook Has Gained This Revenue by Acting as a Data Broker—and Partnering with Other Data Brokers-----	133
J.	The Content and Information About Its Users That Facebook Has Shared With Third Parties Has Allowed Advertisers and Political Operatives to Harass and Discriminate Against Them -----	136
1.	Facebook Users Did Not Understand that Their Content and Information Would Be Used for Psychographic Marketing -----	136
2.	The Features That Facebook Has Offered Advertisers Allow Extraordinarily Harmful and Invasive Forms of Psychographic Marketing -----	138
3.	The Aggregation of User Content Via Third Parties, Including Device Makers and App Developers, Has Greatly Accelerated the Potential for Data Abuse-----	145
V.	PRIMA FACIE CASE OF INJURY AND DAMAGES -----	145
A.	Plaintiffs Suffered Harm as a Direct Result of Facebook’s Conduct-----	145
VI.	PLAINTIFFS COULD NOT HAVE DISCOVERED THEIR CLAIMS UNTIL 2018. -----	153
VII.	CHOICE OF LAW -----	155
VIII.	CLASS ACTION ALLEGATIONS-----	155
IX.	CAUSES OF ACTION-----	169
A.	Prioritized Claims -----	169
Claim I.	Violation of the Stored Communications Act (“SCA”), 18 U.S.C. §§ 2701 <i>et seq.</i> -----	169
Claim II.	Violation of Video Privacy Protection Act, 18 U.S.C. § 2710 -----	173
Claim III.	Deceit by Concealment or Omission Cal. Civ. Code §§ 1709 & 1710 -----	174
Claim IV.	Invasion of Privacy – Intrusion into Private Affairs -----	180

Claim V.	Invasion of Privacy – Public Disclosure of Private Facts ---	181
Claim VI.	Breach of Contract-----	182
Claim VII.	Negligence and Gross Negligence-----	185
Claim VIII.	Violations of the California Unfair Competition Law Cal. Bus. & Prof. Code §§ 17200 <i>et seq.</i> -----	189
Claim IX.	Violation of Article I, Section 1 of the California Constitution-----	193
Claim X.	Violation of California Common Law Right of Publicity---	195
Claim XI.	Breach of the Implied Covenant of Good Faith and Fair Dealing-----	196
Claim XII.	Quantum Meruit to Recover Sums Had by Unjust Enrichment -----	198
B.	Priority Consumer Protection Act Claims Alleged in the Alternative -----	200
Claim XIII.	Violations of the Alabama Deceptive Trade Practices Act Ala. Code §§ 8-19-1 <i>et seq.</i> (2018)-----	200
Claim XIV.	Violations of the Colorado Consumer Protection Act Colo. Rev. Stat. Ann. §§ 6-1-101 <i>et seq.</i> -----	202
Claim XV.	Violations of the Illinois Consumer Fraud and Deceptive Business Practices Act 815 Ill. comp. stat. Ann. §§ 505 <i>et seq.</i> -----	205
Claim XVI.	Violations of the Iowa Private Right of Action for Consumer Frauds Act Iowa Code Ann. § 714H -----	207
Claim XVII.	Violations of the Kansas Consumer Protection Act Kan. Stat. Ann. §§ 50-623 <i>et seq.</i> -----	209
Claim XVIII.	Violations of the Michigan Consumer Protection Act Mich. Comp. Laws Ann. §§ 445.901 <i>et seq.</i> -----	212
Claim XIX.	Violations of the New York General Business Law N.Y. Gen. Bus. Law §§ 349 <i>et seq.</i> -----	214
Claim XX.	Violations of the Washington Consumer Protection Act Wash. Rev. Code Ann. §§ 19.86.010 <i>et seq.</i> -----	216
Claim XXI.	Violations of the West Virginia Consumer Credit and Protection Act-----	218
C.	Non-Prioritized Claims-----	223
Claim XXII.	Racketeer Influence and Corrupt Organizations Act, 18 U.S.C. § 1962(c)-----	223
Claim XXIII.	Misappropriation of Valuable Property-----	226

Claim XXIV.	Fraudulent Misrepresentation -----	227
Claim XXV.	Negligent Misrepresentation -----	228
Claim XXVI.	Trespass to Personal Property-----	229
Claim XXVII.	Conversion-----	230
Claim XXVIII.	Unlawful Interception of Communications – 11 Del. Code § 2401 -----	230
Claim XXIX.	Violation of California Consumer Record Act-----	232
Claim XXX.	Violation of California Invasion of Privacy Act (Cal. Pen. Code § 637.7) -----	233
Claim XXXI.	Violation of the California Consumers Legal Remedies Act	235
Claim XXXII.	Violation of California’s Computer Data Access and Fraud Act-----	236
Claim XXXIII.	Violations of Common Law Right to Privacy in the Following States: Alabama; Arizona; Colorado; Florida; Georgia; Idaho; Indiana; Iowa; Kansas; Maryland; Michigan; Missouri; Ohio; Oklahoma; Pennsylvania; Tennessee; Texas; Washington; West Virginia; and Wisconsin-----	237
Claim XXXIV.	Violations of Alabama Right of Publicity Statute, Ala. Code § 6-5-772-----	238
Claim XXXV.	Violations of Florida Unauthorized Publication Statute, Fla. State Code § 540.08 -----	239
Claim XXXVI.	Violations of Illinois Right of Publicity Statute, Ill. Comp. Stat. § 1075/10 -----	240
Claim XXXVII.	Violations of Indiana Rights of Publicity Code, Ind. Code § 32-36-1-8 -----	241
Claim XXXVIII.	Violations of New York Right to Privacy Statute, N.Y. Civ. Rights Law § 51	242
Claim XXXIX.	Violations of Ohio Right of Publicity Statute, Ohio Code § 2741.02-----	243
Claim XL.	Violations of Oklahoma Rights of Publicity Statute, Okl. St. § 1449 -----	244
Claim XLI.	Violations of Pennsylvania Unauthorized Use Statute, 42 Pa. Stat. § 8316 -----	245
Claim XLII.	Violations of Tennessee Protection of Personal Rights Statute T.C.A. § 47-25-1105 -----	246
Claim XLIII.	Violations of Virginia Unauthorized Use Statute, Va. Code § 8.01-40-----	247



Claim XLIV.	Violations of Washington Personality Right Statue, Wash. Code § 63.60.050 -----	248
Claim XLV.	Violations of Wisconsin Right of Publicity Statute, Wis. Stat. § 995.50-----	249
Claim XLVI.	Violations of California Right of Publicity Statute, Cal. Civil Code § 3344 -----	250
Claim XLVII.	Violations of the Fair Credit Reporting Act 15 U.S.C. §§ 1681 <i>et seq.</i> -----	251
Claim XLVIII.	Unlawful Interception of Communications, 11 Del. Code § 2401 -----	253
Claim XLIX.	Violation of New Jersey Consumer Fraud Act, N.J. Stat. Ann. §§ 56:8-1 <i>et seq.</i> -----	254
Claim L.	Intentional Misrepresentation -----	256
X.	PRAYER FOR RELIEF -----	257
XI.	DEMAND FOR JURY TRIAL -----	257

**TABLE OF AUTHORITIES**

	<b>Page(s)</b>
<b>Statutes</b>	
15 U.S.C. § 1681 .....	249, 250
18 U.S.C. § 1961 .....	221, 223
18 U.S.C. § 2501 .....	156, 169
18 U.S.C. § 2510 .....	<i>passim</i>
18 U.S.C. § 2701 .....	<i>passim</i>
18 U.S.C. § 2702 .....	<i>passim</i>
18 U.S.C. § 2707 .....	167, 168, 169, 170
18 U.S.C. § 2710 .....	<i>passim</i>
18 U.S.C. § 2711 .....	156, 169
28 U.S.C. § 1331 .....	5
28 U.S.C. § 1332 .....	5
28 U.S.C. § 1367 .....	5
28 U.S.C. § 1391 .....	5
28 U.S.C. § 1407 .....	167
Cal. Bus. & Prof. Code §§ 17200 <i>et seq.</i> .....	156, 187
California Civil Code § 1021.5 .....	231
California Civil Code § 1709 .....	172, 174, 189
California Civil Code § 1710 .....	172, 189
California Civil Code § 1770(a) .....	233
California Civil Code § 1782(a) .....	233
California Civil Code § 1798 .....	229, 230, 231
California Civil Code § 3344 .....	248, 249

California Penal Code § 502 .....	234
California Penal Code § 630 .....	231
California Penal Code § 637.7(a).....	232

Plaintiffs Tonya Smith, Paige Grays, Anthony Bell, Olivia Johnston, Jordan O'Hara, Juliana Watson, Shelly Forman, Bridgett Burk, Charnae Tutt, Brendan Carr, Kimberly Robertson, Samuel Armstrong, Mitch Staggs, Dustin Short, Barbara Vance-Guerbe, Jason Ariciu, William Lloyd, Cheryl Senko, Ian Miller, Steven Akins, Tyler King, Gretchen Maxwell, Scott Schinder, Mary Beth Grisi, Suzie Haslinger, Terry Fischer, Taunna Jarvimaki, Sandra Adkins, Ashley Kmiecik, Scott McDonnell, Tabielle Holsinger, James Tronka, Bridget Peters, and John Doe, individually and as representatives of Classes of similarly situated persons, by their undersigned counsel, allege as follows:

### I. INTRODUCTION

1. Just fourteen years after its founding, Facebook, Inc. (“Facebook” or the “Company”) has become one of the world’s largest companies. Its reach today is immense. More than 2.2 billion people around the world use its social networking platform to connect with each other.<sup>1</sup> It is no exaggeration that Facebook’s connectivity has transformed the world. For many, it has become an indispensable tool in keeping up with friends, running a business or advancing in a career, and remaining informed about the world.

2. Valued at more than \$473 billion, Facebook made more than \$40 billion in revenue last year. Despite Facebook’s origins as a social networking company, that revenue flows not from user fees, but from allowing third parties to target its users with advertising and messaging.

3. Users have been generally aware, of course, that advertising revenue drives Facebook’s business model. What users did not know until March of 2018, and what Facebook did not properly disclose, was that Facebook has enabled the wholesale disclosure of users’

---

<sup>1</sup> “If Facebook were a country, it would have the largest population on earth. More than 2.2 billion people, about a third of humanity, log in at least once a month. That user base has no precedent in the history of American enterprise. Fourteen years after it was founded, in Zuckerberg’s dorm room, Facebook has as many adherents as Christianity.” Evan Osnos, *Can Mark Zuckerberg Fix Facebook Before It Breaks Democracy?*, New Yorker (Sept. 17, 2018), <https://www.newyorker.com/magazine/2018/09/17/can-mark-zuckerberg-fix-facebook-before-it-breaks-democracy>.

content and information<sup>2</sup> to third parties, even when users had not chosen to share it with them. Nor did they know that Facebook has done almost nothing to prevent those third parties from misusing the content and information themselves, or from disclosing that content and information to still other entities.

4. These aspects of Facebook’s business became public in March 2018, when a journalist uncovered that Cambridge Analytica, LLC (“Cambridge Analytica”), a British political consulting firm, paid a Facebook app developer to collect and analyze the content and information of approximately 87 million Facebook users (the “Cambridge Analytica Scandal” or “Scandal”).

5. Cambridge Analytica then used this content and information to influence voters in eleven states in the 2016 U.S. elections by cross-referencing users’ Facebook content and information with voter identification data. Using what it learned about them from Facebook, Cambridge Analytica was able to identify voters by name and target them with individually crafted messages about political candidates.

6. Cambridge Analytica was able to accomplish this by purchasing Facebook user data from an app developer. The app developer, in turn, had been allowed access to specific Facebook users’ content and information. This access was not isolated or unusual. Facebook has had partnership agreements with businesses large and small to share content and information—without user consent or notification—dating back to 2007. In fact, Facebook created whole systems that allowed third parties—not just applications that used Facebook, but also mobile carriers, software makers, security firms and device makers—to access users’ content and information. These were not data breaches. This was intentional.

7. The access that Facebook allowed these third parties was extensive. Facebook

---

<sup>2</sup> As used here, “content and information” means “content” and “information” as Facebook’s Statements of Rights and Responsibilities have defined those terms. In brief, Facebook has generally used “information” to mean facts and other information about Facebook users, including their actions they take, and “content” to mean anything users post on Facebook that would not be included in the definition of “information.” In addition, as used in this complaint, the terms include both personally identifiable content and information *and* anonymized content and information that is capable of being de-anonymized. For more details, see *infra* ¶¶ 223-224.

allowed these third parties to access not only the content and information of the user who had installed the application, but also the content and information that that user's *friends* had shared with her. Third parties were allowed access not by users themselves, but when friends engaged with the third party, be it an app, a phone, or a website.

8. Despite creating these means of access for third parties, Facebook was astonishingly reckless in monitoring them. Facebook never audited any of the app developers to whom it gave access. And once users' content and information was in the hands of undisclosed third parties, Facebook did nothing to ensure that it went no further. In fact, when advised in 2015 that Cambridge Analytica had illegally purchased users' content and information, Facebook did not take steps to inform users or to confirm that the data Cambridge Analytica paid for was destroyed. It has done so now only in the wake of regulatory and governmental outrage.

9. Facebook has never properly informed users about the access it gave third parties. Worse, it misled users on the subject. For while it extolled the supposedly tight control users could wield over what they shared with others, the instruments it provided to users to exert that control were profoundly confusing. Facebook provided "Privacy Settings" to users, and made them prominent and accessible. But the Privacy Settings did not control the information and content that third parties could access. They did not contain any privacy control specifically for mobile carriers like Blackberry, for example—which means that Blackberry had access to the content and information that users shared with friends who had downloaded the Facebook app on their Blackberry. For applications, access was governed by controls called "App Settings"—controls that Facebook buried deep in a maze of webpages. But by default, the App Settings allowed users' content and information to be shared even when a user's friend uploaded an application. Short of deleting a Facebook account, the only fool-proof method for preventing data collection is to set *all* settings to private, so that not even your friends can view your content and information. That, of course, defeats the purpose of joining Facebook, sold to users as a social networking platform.

10. Similarly confusing were the tangle of various documents that purported to

govern the relationship between Facebook and its users. These documents were difficult to access on Facebook's website, and equally difficult to understand—and on top of that, Facebook constantly changed them without notice. None of these documents meaningfully disclosed the access that Facebook granted to third parties, or how third parties could use that access.

11. One of the few things that *is* clear from the documents is Facebook's promise not to share its users' content and information with advertisers. Facebook also told users that they owned and controlled their content and information. As noted above, Facebook broke that promise, and shared it with companies like mobile carriers and app developers who of course advertise.

12. But the harms that Facebook has inflicted upon users arise from more than just Facebook's unauthorized disclosure of content and information with third parties. Those harms arise also from the ease with which third parties can de-anonymize the data, tying it to specific individuals by name. This creates a substantial and imminent risk of identity theft, fraud, stalking, scams, unwanted texts, emails and even hacking. The fundamental pieces of a Facebook profile—names, phone numbers, email addresses and the kind of corroborating personal information used for passwords and security questions—serve as critical starter kits for identity theft and other malicious online activity. Experts agree, for example, that users can be individually targeted in an attempt to perpetuate voter fraud, medical fraud, and other harms. The disclosure of this content “allow[s] bad actors to tie raw data to people's real identities and build fuller profiles of them.”<sup>3</sup> Thus, this is not a case of the simple theft of social security numbers or credit card numbers. Facebook users suffered concrete injury in ways that transcend a normal data breach injury.

13. Moreover, from a marketing perspective, the ability to de-anonymize and analyze user data allows consumers to be personally, rather than generally, targeted. This is called

---

<sup>3</sup> Craig Timberg et. al., *Facebook: 'Malicious Actors' Used its Tools to Discover Identities and Collect Data on a Massive Global Scale*, Wash. Post (Apr. 4, 2018), [https://www.washingtonpost.com/news/the-switch/wp/2018/04/04/facebook-said-the-personal-data-of-most-its-2-billion-users-has-been-collected-and-shared-with-outsiders/?noredirect=on&utm\\_term=.4e5be0d26e2b](https://www.washingtonpost.com/news/the-switch/wp/2018/04/04/facebook-said-the-personal-data-of-most-its-2-billion-users-has-been-collected-and-shared-with-outsiders/?noredirect=on&utm_term=.4e5be0d26e2b).

“psychographic marketing.” With the advent of psychographic marketing, users’ content and information is analyzed and studied by marketing and political campaigns, all in an effort to deliver targeted content that will trigger them to act. Indeed, Cambridge Analytica exploited users’ information to target individual voters by name with content tailored to their predicted psychological proclivities. Facebook and other data brokers collect data dossiers of Facebook users based on this aggregated data that make assumptions about health, financial risk, employability and other factors. Brokers, like Facebook, then make that data accessible to third parties to target people based on analysis of their temperament and vulnerabilities—unknownst to the targets, who, in this case, were Facebook users.

14. Plaintiffs and the Classes seek to be put back in the position they would occupy had Facebook properly disclosed its activities or simply not engaged in them at all. This lawsuit seeks an audit and disclosure, a change of Facebook’s default settings, compensation for intrusions into privacy on an unprecedented level, and benefit-of-the-bargain damages for users who did not understand what was taken from them and how Facebook has profited, among other relief.

## **II. JURISDICTION, VENUE, AND CHOICE OF LAW**

15. Pursuant to 28 U.S.C. § 1331, this Court has original subject matter jurisdiction over the claims that arise under the Stored Communications Act, 18 U.S.C. §§ 2701 *et seq.* and the Video Privacy Protection Act, 18 U.S.C. § 2710.

16. This Court also has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367.

17. In addition to federal question jurisdiction, this Court also has diversity jurisdiction pursuant to 28 U.S.C. § 1332(d) under the Class Action Fairness Act (“CAFA”), because the amount in controversy exceeds \$5,000,000, exclusive of interest and costs, and at least one Class Member is a citizen of a state different from Defendants.

18. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because Defendants do business in and are subject to personal jurisdiction in this District. Venue is also proper



because a substantial part of the events or omissions giving rise to the claim occurred in or emanated from this District.

19. The relevant terms of Plaintiffs' contracts with Facebook provide that the exclusive venues for litigating any claim with Facebook are either the United States District Court for the Northern District of California or a state court located in San Mateo County. These contracts also provided that all claims that might arise between the user and Facebook would be governed by the laws of California, without regard to conflict-of-law provisions.

20. The venue provision provides an additional reason that venue is proper in this District. The choice-of-law provision establishes that California law applies to Plaintiffs' and all Class Members' claims.

### III. PARTIES

#### A. Plaintiffs

21. **Plaintiff Tonya Smith** is a citizen and resident of the State of Alabama. Plaintiff Smith created her Facebook account approximately eleven years ago. Plaintiff Smith maintains her Facebook account to the present day. Plaintiff Smith has accessed her Facebook account from a mobile phone, a Chromebook, and a personal computer. Plaintiff Smith has watched and "liked" videos on Facebook and has also "liked" pages on Facebook that contain videos. Plaintiff Smith also uses Facebook messenger and/or instant messaging through Facebook. Plaintiff Smith shared content and information with Facebook, which she expected Facebook to protect and secure against access by or disclosure to unauthorized parties. Plaintiff Smith confirmed on Facebook that her content and information may have been "shared" with and "misused" by the This Is Your Digital Life app, because one of Plaintiff Smith's Facebook friends downloaded the This Is Your Digital Life app. Plaintiff Smith was not aware of and did not consent to the sharing of her content and information with the This Is Your Digital Life app. Moreover, Plaintiff Smith did not consent to any third-parties accessing her content and information through her Facebook friends and had no knowledge that Facebook had authorized this disclosure of her content and information without her consent.

22. During the 2016 U.S. Presidential election, Plaintiff Smith frequently received political advertisements while using Facebook. On information and belief, Plaintiff Smith was targeted by some or all of these advertisements as a result of the Cambridge Analytica Scandal. As a result of the release of her content and information, Plaintiff Smith has suffered emotional distress, including anxiety, concern, and unease about unauthorized parties viewing and using her content and information for improper purposes, such as identity theft and fraud as well as further intruding upon Plaintiff Smith's private affairs and concerns, as detailed herein. Plaintiff Smith fears that she is at risk of identity theft and fraud, and now spends approximately thirty minutes each month monitoring her credit, bank, and other account statements for evidence of identity theft and fraud, and anticipates continuing to do so for the foreseeable future.

23. **Plaintiff Paige Grays** is a citizen and resident of the State of Arizona. Plaintiff Grays created her Facebook account approximately seven years ago. Plaintiff Grays maintains her Facebook account to the present day. Plaintiff Grays has accessed her Facebook account from a mobile phone and a personal computer. Plaintiff Grays has watched and "liked" videos on Facebook and has also "liked" pages on Facebook that contain videos. Plaintiff Grays shared content and information with Facebook, which she expected Facebook to protect and secure against access by or disclosure to unauthorized parties. Plaintiff Grays confirmed on Facebook that her content and information "was likely shared with" and may have been "misused" by the This Is Your Digital Life app, because one of Plaintiff Grays' Facebook friends downloaded the This Is Your Digital Life app. Plaintiff Grays was not aware of and did not consent to the sharing of her content and information with the This Is Your Digital Life app. Moreover, Plaintiff Grays did not consent to any third-parties accessing her content and information through her Facebook friends and had no knowledge that Facebook had authorized this disclosure of her content and information without her consent.

24. During the 2016 U.S. Presidential election, Plaintiff Grays frequently received political advertisements while using Facebook. On information and belief, Plaintiff Grays was targeted by some or all of these advertisements as a result of the Cambridge Analytica Scandal.

As a result of the release of her content and information, Plaintiff Grays has suffered emotional distress, including anxiety, concern, and unease about unauthorized parties viewing and using her content and information for improper purposes, such as identity theft and fraud as well as further intruding upon Plaintiff Grays' private affairs and concerns, as detailed herein. Plaintiff Grays fears that she is at risk of identity theft and fraud.

25. **Plaintiff Anthony Bell** is a citizen and resident of the State of California. Plaintiff Bell created his Facebook account approximately thirteen years ago. Plaintiff Bell maintains his Facebook account to the present day. Plaintiff Bell has accessed his Facebook account from a mobile phone and a personal computer. Plaintiff Bell has watched and "liked" videos on Facebook and has also "liked" pages on Facebook that contain videos. Plaintiff Bell also uses Facebook messenger and/or instant messaging through Facebook. Plaintiff Bell shared content and information with Facebook, which he expected Facebook to protect and secure against access by or disclosure to unauthorized parties. Plaintiff Bell confirmed on Facebook that his content and information may have been "shared" with and "misused" by the This Is Your Digital Life app, because one of Plaintiff Bell's Facebook friends downloaded the This Is Your Digital Life app. Plaintiff Bell was not aware of and did not consent to the sharing of his content and information with the This Is Your Digital Life app. Moreover, Plaintiff Bell did not consent to any third-parties accessing his content and information through his Facebook friends and had no knowledge that Facebook had authorized this disclosure of his content and information without his consent.

26. During the 2016 U.S. Presidential election, Plaintiff Bell frequently received political advertisements while using Facebook. On information and belief, Plaintiff Bell was targeted by some or all of these advertisements as a result of the Cambridge Analytica Scandal. As a result of the release of his content and information, Plaintiff Bell has suffered emotional distress, including anxiety, concern, and unease about unauthorized parties viewing and using his content and information for improper purposes, such as identity theft and fraud as well as further intruding upon Plaintiff Bell's private affairs and concerns, as detailed herein. Plaintiff Bell fears

that he is at risk of identity theft and fraud, and now spends approximately five hours each month monitoring his credit, bank, and other account statements for evidence of identity theft and fraud, and anticipates continuing to do so for the foreseeable future. Because of his heightened risk of identity theft and fraud, Plaintiff Bell has purchased credit monitoring and identity theft protection services, and anticipates continuing to pay for such services for the foreseeable future.

27. **Plaintiff Olivia Johnston** is a citizen and resident of the State of California. Plaintiff Johnston created her Facebook account approximately seven years ago. Plaintiff Johnston maintains her Facebook account to the present day. Plaintiff Johnston has accessed her Facebook account from a mobile phone and a personal computer. Plaintiff Johnston has watched and “liked” videos on Facebook and has also “liked” pages on Facebook that contain videos. Plaintiff Johnston also uses Facebook messenger and/or instant messaging through Facebook. Plaintiff Johnston shared content and information with Facebook, which she expected Facebook to protect and secure against access by or disclosure to unauthorized parties. In approximately April 2018, Plaintiff Johnston learned that millions of Facebook users’ content and information may have been obtained by the This Is Your Digital Life app, because Plaintiff Johnston downloaded the This Is Your Digital Life app. Plaintiff Johnston was not aware of and did not consent to the sharing of her content and information with the This Is Your Digital Life app. Moreover, Plaintiff Johnston did not consent to any third-parties accessing her content and information through her Facebook friends and had no knowledge that Facebook had authorized this disclosure of her content and information without her consent.

28. As a result of this concern for the security of her content and information, Plaintiff Johnston has suffered emotional distress, including anxiety, concern, and unease about unauthorized parties viewing and using her content and information for improper purposes, such as identity theft and fraud as well as further intruding upon Plaintiff Johnston’s private affairs and concerns, as detailed herein. Plaintiff Johnston fears that she is at risk of identity theft and fraud.

29. **Plaintiff Jordan O'Hara** is a citizen and resident of the State of California. Plaintiff O'Hara created his Facebook account approximately ten years ago. Plaintiff O'Hara maintains his Facebook account to the present. Plaintiff O'Hara has accessed his Facebook account from a mobile phone and a personal computer. Plaintiff O'Hara has watched and "liked" videos on Facebook and has also "liked" pages on Facebook that contain videos. Plaintiff O'Hara also uses Facebook messenger and/or instant messaging through Facebook. Plaintiff O'Hara shared content and information with Facebook, which he expected Facebook to protect and secure against access by or disclosure to unauthorized parties. Plaintiff O'Hara confirmed on Facebook that his content and information may have been "shared" with and "misused" by the This Is Your Digital Life app, because one of Plaintiff O'Hara's Facebook friends downloaded the This Is Your Digital Life app. Plaintiff O'Hara was not aware of and did not consent to the sharing of his content and information with the This Is Your Digital Life app. Moreover, Plaintiff O'Hara did not consent to any third-parties accessing his content and information through his Facebook friends and had no knowledge that Facebook had authorized this disclosure of his content and information without his consent.

30. During the 2016 U.S. Presidential election, Plaintiff O'Hara frequently received political advertisements while using Facebook. On information and belief, Plaintiff O'Hara was targeted by some or all of these advertisements as a result of the Cambridge Analytica Scandal. As a result of the release of his content and information, Plaintiff O'Hara has suffered emotional distress, including anxiety, concern, and unease about unauthorized parties viewing and using his content and information for improper purposes, such as identity theft and fraud as well as further intruding upon Plaintiff O'Hara's private affairs and concerns, as detailed herein. Plaintiff O'Hara fears that he is at risk of identity theft and fraud, and now spends approximately one hour each month monitoring his credit, bank, and other account statements for evidence of identity theft and fraud, and anticipates continuing to do so for the foreseeable future. Because of his heightened risk of identity theft and fraud, Plaintiff O'Hara has obtained credit monitoring and

identity theft protection services as a result of his status as a former member of the armed services, and anticipates continuing to use services for the foreseeable future.

31. **Plaintiff Juliana Watson** is a citizen and resident of the State of California. Plaintiff Watson created her Facebook account approximately nine years ago. Plaintiff Watson maintains her Facebook account to the present day. Plaintiff Watson has accessed her Facebook account from a mobile phone and a personal computer. Plaintiff Watson has watched and “liked” videos on Facebook and has also “liked” pages on Facebook that contain videos. Plaintiff Watson also uses Facebook messenger and/or instant messaging through Facebook. Plaintiff Watson shared content and information with Facebook, which she expected Facebook to protect and secure against access by or disclosure to unauthorized parties. Plaintiff Watson confirmed on Facebook that her content and information “was likely shared with” the This Is Your Digital Life app, because one of Plaintiff Watson’s Facebook friends downloaded the This Is Your Digital Life app. Plaintiff Watson was not aware of and did not consent to the sharing of her content and information with the This Is Your Digital Life app. Moreover, Plaintiff Watson did not consent to any third-parties accessing her content and information through her Facebook friends and had no knowledge that Facebook had authorized this disclosure of her content and information without her consent.

32. During the 2016 U.S. Presidential election, Plaintiff Watson frequently received political advertisements while using Facebook. On information and belief, Plaintiff Watson was targeted by some or all of these advertisements as a result of the Cambridge Analytica Scandal. As a result of the release of her content and information, Plaintiff Watson has suffered emotional distress, including anxiety, concern, and unease about unauthorized parties viewing and using her content and information for improper purposes, such as identity theft and fraud as well as further intruding upon Plaintiff Watson’s private affairs and concerns, as detailed herein. Plaintiff Watson fears that she is at risk of identity theft and fraud.

33. **Plaintiff Shelly Forman** is a citizen and resident of the State of Georgia. Prior to August 1, 2018, Plaintiff Forman was at all relevant times a resident of the State of Colorado.

Plaintiff Forman created her Facebook account approximately ten years ago. Plaintiff Forman maintains her Facebook account to the present day. Plaintiff Forman has accessed her Facebook account from a mobile phone and a personal computer. Plaintiff Forman has watched and “liked” videos on Facebook and has also “liked” pages on Facebook that contain videos. Plaintiff Forman also uses Facebook messenger and/or instant messaging through Facebook. Plaintiff Forman shared content and information with Facebook, which she expected Facebook to protect and secure against access by or disclosure to unauthorized parties. Plaintiff Forman confirmed on Facebook that her content and information may have been “shared” with and “misused” by the This Is Your Digital Life app, because one of Plaintiff Forman’s Facebook friends downloaded the This Is Your Digital Life app. Plaintiff Forman was not aware of and did not consent to the sharing of her content and information with the This Is Your Digital Life app. Moreover, Plaintiff Forman did not consent to any third-parties accessing her content and information through her Facebook friends and had no knowledge that Facebook had authorized this disclosure of her content and information without her consent.

34. During the 2016 U.S. Presidential election, Plaintiff Forman frequently received political advertisements while using Facebook. On information and belief, Plaintiff Forman was targeted by some or all of these advertisements as a result of the Cambridge Analytica Scandal. As a result of the release of her content and information, Plaintiff Forman has suffered emotional distress, including anxiety, concern, and unease about unauthorized parties viewing and using her content and information for improper purposes, such as identity theft and fraud as well as further intruding upon Plaintiff Forman’s private affairs and concerns, as detailed herein. Plaintiff Forman fears that she is at risk of identity theft and fraud, and now spends approximately one to two hours each month monitoring her credit, bank, and other account statements for evidence of identity theft and fraud, and anticipates continuing to do so for the foreseeable future.

35. **Plaintiff Scott McDonnell** is a citizen and a resident of the State of Connecticut. Plaintiff McDonnell created his Facebook account approximately ten years ago. Plaintiff

McDonnell maintains his Facebook account to the present day. Plaintiff McDonnell has accessed his Facebook account from a mobile phone and a personal computer. Plaintiff McDonnell has watched and “liked” videos on Facebook and has also “liked” pages on Facebook that contain videos. Plaintiff McDonnell also uses Facebook messenger and/or instant messaging through Facebook. Plaintiff McDonnell shared content and information with Facebook, which he expected Facebook to protect and secure against access by or disclosure to unauthorized parties. In approximately April 2018, Plaintiff McDonnell received notice from Facebook that his Personal Information may have been “shared” with and “misused” by the This Is Your Digital Life app, because one of Plaintiff McDonnell’s Facebook friends downloaded the This Is Your Digital Life app. Plaintiff McDonnell was not aware of and did not consent to the sharing of his content and information with the This Is Your Digital Life app. Moreover, Plaintiff McDonnell did not consent to any third-parties accessing his content and information through his Facebook friends and had no knowledge that Facebook had authorized this disclosure of his content and information without his consent.

36. During the 2016 U.S. Presidential election, Plaintiff McDonnell frequently received political advertisements while using Facebook. On information and belief, Plaintiff McDonnell was targeted by some or all of these advertisements as a result of the Cambridge Analytica Scandal. As a result of the release of his content and information, Plaintiff McDonnell has suffered emotional distress, including anxiety, concern, and unease about unauthorized parties viewing and using his content and information for improper purposes, such as identity theft and fraud as well as further intruding upon Plaintiff McDonnell’s private affairs and concerns, as detailed herein. Plaintiff McDonnell fears that he is at risk of identity theft and fraud, and now spends approximately two hours each month monitoring his credit, bank, and other account statements for evidence of identity theft and fraud, and anticipates continuing to do so for the foreseeable future. Because of his heightened risk of identity theft and fraud, Plaintiff McDonnell has purchased credit monitoring and identity theft protection services, for which he



pays approximately \$40 per month, and anticipates continuing to pay for such services for the foreseeable future.

37. **Plaintiff Bridgett Burk** is a citizen and resident of the State of Florida. Plaintiff Burk created her Facebook account approximately twelve years ago. Plaintiff Burk maintains her Facebook account to the present day. Plaintiff Burk has accessed her Facebook account from a mobile phone and a personal computer. Plaintiff Burk has watched and “liked” videos on Facebook and has also “liked” pages on Facebook that contain videos. Plaintiff Burk also uses Facebook messenger and/or instant messaging through Facebook. Plaintiff Burk shared content and information with Facebook, which she expected Facebook to protect and secure against access by or disclosure to unauthorized parties. Plaintiff Burk confirmed on Facebook that her content and information may have been “shared” with and “misused” by the This Is Your Digital Life app, because one of Plaintiff Burk’s Facebook friends downloaded the This Is Your Digital Life app. Plaintiff Burk was not aware of and did not consent to the sharing of her content and information with the This Is Your Digital Life app. Moreover, Plaintiff Burk did not consent to any third-parties accessing his content and information through her Facebook friends and had no knowledge that Facebook had authorized this disclosure of her content and information without her consent.

38. As a result of the release of her content and information, Plaintiff Burk has suffered emotional distress, including anxiety, concern, and unease about unauthorized parties viewing and using her content and information for improper purposes, such as identity theft and fraud as well as further intruding upon Plaintiff Burk’s private affairs and concerns, as detailed herein. Plaintiff Burk fears that she is at risk of identity theft and fraud, and now spends approximately thirty minutes each month monitoring her credit, bank, and other account statements for evidence of identity theft and fraud, and anticipates continuing to do so for the foreseeable future.

39. **Plaintiff Charnae Tutt** is a citizen and resident of the State of Georgia. Plaintiff Tutt created her Facebook account approximately ten years ago. Plaintiff Tutt maintains her

Facebook account to the present day. Plaintiff Tutt has accessed her Facebook account from a mobile phone and a personal computer. Plaintiff Tutt has watched and “liked” videos on Facebook and has also “liked” pages on Facebook that contain videos. Plaintiff Tutt also uses Facebook messenger and/or instant messaging through Facebook. Plaintiff Tutt shared content and information with Facebook, which she expected Facebook to protect and secure against access by or disclosure to unauthorized parties. Plaintiff Tutt confirmed on Facebook that her content and information may have been “shared” with and “misused” by the My Personality app. Plaintiff Tutt was not aware of and did not consent to the sharing of her content and information with the My Personality app. Moreover, Plaintiff Tutt did not consent to any third-parties accessing her content and information through her Facebook friends and had no knowledge that Facebook had authorized this disclosure of her content and information without her consent.

40. During the 2016 U.S. Presidential election, Plaintiff Tutt frequently received political advertisements while using Facebook. On information and belief, Plaintiff Tutt was targeted by some or all of these advertisements as a result of the Cambridge Analytica Scandal. As a result of the release of her content and information, Plaintiff Tutt has suffered emotional distress, including anxiety, concern, and unease about unauthorized parties viewing and using her content and information for improper purposes, such as identity theft and fraud as well as further intruding upon Plaintiff Tutt’s private affairs and concerns, as detailed herein. Plaintiff Tutt fears that she is at risk of identity theft and fraud, and now spends approximately five hours each month monitoring her credit, bank, and other account statements for evidence of identity theft and fraud, and anticipates continuing to do so for the foreseeable future.

41. **Plaintiff Tabielle Holsinger** is a citizen and a resident of the State of Idaho. Plaintiff Holsinger created her Facebook account approximately nine years ago. Plaintiff Holsinger maintains her Facebook account to the present day. Plaintiff Holsinger has accessed her Facebook account from a mobile phone. Plaintiff Holsinger has watched and “liked” videos on Facebook and has also “liked” pages on Facebook that contain videos. Plaintiff Holsinger also uses Facebook messenger and/or instant messaging through Facebook. Plaintiff Holsinger shared

content and information with Facebook, which she expected Facebook to protect and secure against access by or disclosure to unauthorized parties. Plaintiff Holsinger confirmed on Facebook that her content and information “was likely shared with” and may have been “misused” by the This Is Your Digital Life app, because one of Plaintiff Holsinger’s Facebook friends downloaded the This Is Your Digital Life app. Plaintiff Holsinger was not aware of and did not consent to the sharing of her content and information with the This Is Your Digital Life app. Moreover, Plaintiff Holsinger did not consent to any third-parties accessing her content and information through her Facebook friends and had no knowledge that Facebook had authorized this disclosure of her content and information without her consent.

42. During the 2016 U.S. Presidential election, Plaintiff Holsinger frequently received political advertisements while using Facebook. On information and belief, Plaintiff Holsinger was targeted by some or all of these advertisements as a result of the Cambridge Analytica Scandal. As a result of the release of her content and information, Plaintiff Holsinger has suffered emotional distress, including anxiety, concern, and unease about unauthorized parties viewing and using her content and information for improper purposes, such as identity theft and fraud as well as further intruding upon Plaintiff Holsinger’s private affairs and concerns, as detailed herein. Plaintiff Holsinger fears that she is at risk of identity theft and fraud, and now spends approximately four hours each month monitoring her credit, bank, and other account statements for evidence of identity theft and fraud, and anticipates continuing to do so for the foreseeable future.

43. **Plaintiff Brendan Carr** is a citizen and resident of the State of Illinois. Plaintiff Carr created his Facebook account approximately thirteen years ago. Plaintiff Carr maintains his Facebook account to the present day. Plaintiff Carr has accessed his Facebook account from a mobile phone and a personal computer. Plaintiff Carr has watched and “liked” videos on Facebook and has also “liked” pages on Facebook that contain videos. Plaintiff Carr also uses Facebook messenger and/or instant messaging through Facebook. Plaintiff Carr shared content and information with Facebook, which he expected Facebook to protect and secure against

access by or disclosure to unauthorized parties. In approximately April 2018, Plaintiff Carr received notice from Facebook that his content and information may have been obtained by the This Is Your Digital Life app, because one of Plaintiff Carr's Facebook friends downloaded the This Is Your Digital Life app. Plaintiff Carr was not aware of and did not consent to the sharing of his content and information with the This Is Your Digital Life app. Moreover, Plaintiff Carr did not consent to any third-parties accessing his content and information through his Facebook friends and had no knowledge that Facebook had authorized this disclosure of his content and information without his consent.

44. During the 2016 U.S. Presidential election, Plaintiff Carr frequently received political advertisements while using Facebook. On information and belief, Plaintiff Carr was targeted by some or all of these advertisements as a result of the Cambridge Analytica Scandal. As a result of the release of his content and information, Plaintiff Carr has suffered emotional distress, including anxiety, concern, and unease about unauthorized parties viewing and using his content and information for improper purposes, such as identity theft and fraud as well as further intruding upon Plaintiff Carr's private affairs and concerns, as detailed herein. Plaintiff Carr fears that he is at risk of identity theft and fraud, and now spends several hours each month monitoring his credit, bank, and other account statements for evidence of identity theft and fraud, and anticipates continuing to do so for the foreseeable future.

45. **Plaintiff John Doe**, a minor, is a citizen and resident of the State of Illinois. Plaintiff Doe created his Facebook account approximately five years ago. Plaintiff Doe maintains his Facebook account to the present day. Plaintiff Doe has accessed his Facebook account from a mobile phone, laptop, and a personal computer. Plaintiff Doe has watched videos on Facebook. Plaintiff Doe also uses Facebook messenger. Plaintiff Doe shared content and information with Facebook, which he expected Facebook to protect and secure against access by or disclosure to unauthorized parties. On information and belief, Plaintiff Doe asserts his content and information was disclosed without his consent to the This Is Your Digital Life app or other third-party apps Facebook is investigating for misusing users' content and information. Plaintiff Doe was not

aware of and did not consent to the sharing of his content and information with the This Is Your Digital Life app or other third parties. Moreover, Plaintiff Doe did not consent to any third-parties accessing his content and information through his Facebook friends and had no knowledge that Facebook had authorized this disclosure of his content and information without his consent.

46. While Doe may not be of sufficient age to understand his exposure, by virtue of his age, he is at greater risk of identity theft, manipulation, fraud, phishing, scams, targeted unwanted and unnecessary advertising, including inappropriate communications. Furthermore, because his content and information was collected before the age of consent, he cannot be expected to understand the gravity of this breach. This does not minimize his risk or threat of future emotional distress, including anxiety, concern and unease about unauthorized parties viewing and using his content and information for improper purposes and further intrusions.

47. **Plaintiff Kimberly Robertson** is a citizen and resident of the State of Illinois. Plaintiff Robertson created her Facebook account approximately nine years ago. Plaintiff Robertson maintains her Facebook account to the present day. Plaintiff Robertson has accessed her Facebook account from a mobile phone and a personal computer. Plaintiff Robertson has watched and “liked” videos on Facebook and has also “liked” pages on Facebook that contain videos. Plaintiff Robertson also uses Facebook messenger and/or instant messaging through Facebook. Plaintiff Robertson shared content and information with Facebook, which she expected Facebook to protect and secure against access by or disclosure to unauthorized parties. Plaintiff Robertson confirmed on Facebook that her content and information may have been “shared” with and “misused” by the This Is Your Digital Life app, because one of Plaintiff Robertson’s Facebook friends downloaded the This Is Your Digital Life app. Plaintiff Robertson was not aware of and did not consent to the sharing of her content and information with the This Is Your Digital Life app. Moreover, Plaintiff Robertson did not consent to any third-parties accessing her content and information through her Facebook friends and had no knowledge that Facebook had authorized this disclosure of her content and information without her consent.

48. As a result of the release of her content and information, Plaintiff Robertson has suffered emotional distress, including anxiety, concern, and unease about unauthorized parties viewing and using her content and information for improper purposes, such as identity theft and fraud as well as further intruding upon Plaintiff Robertson's private affairs and concerns, as detailed herein. Plaintiff Robertson fears that she is at risk of identity theft and fraud, and now spends approximately eight hours each month monitoring her credit, bank, and other account statements for evidence of identity theft and fraud, and anticipates continuing to do so for the foreseeable future.

49. **Plaintiff Samuel Armstrong** is a citizen and resident of the State of Indiana. Plaintiff Armstrong created his Facebook account approximately eleven years ago. Plaintiff Armstrong maintains his Facebook account to the present day. Plaintiff Armstrong has accessed his Facebook account from a mobile phone and a personal computer. Plaintiff Armstrong has watched and "liked" videos on Facebook and has also "liked" pages on Facebook that contain videos. Plaintiff Armstrong also uses Facebook messenger. Plaintiff Armstrong shared content and information with Facebook, which he expected Facebook to protect and secure against access by or disclosure to unauthorized parties. Plaintiff Armstrong confirmed on Facebook that his content and information may have been "shared" with and "misused" by the This Is Your Digital Life app, because one of Plaintiff Armstrong's Facebook friends downloaded the This Is Your Digital Life app. Plaintiff Armstrong was not aware of and did not consent to the sharing of his content and information with the This Is Your Digital Life app. Moreover, Plaintiff Armstrong did not consent to any third-parties accessing his content and information through his Facebook friends and had no knowledge that Facebook had authorized this disclosure of his content and information without his consent.

50. During the 2016 U.S. Presidential election, Plaintiff Armstrong frequently received political advertisements while using Facebook. On information and belief, Plaintiff Armstrong was targeted by some or all of these advertisements as a result of the Cambridge Analytica Scandal. As a result of the release of his content and information, Plaintiff Armstrong

has suffered emotional distress, including anxiety, concern, and unease about unauthorized parties viewing and using his content and information for improper purposes, such as identity theft and fraud as well as further intruding upon Plaintiff Armstrong's private affairs and concerns, as detailed herein. Plaintiff Armstrong fears that he is at risk of identity theft and fraud, and now spends approximately two hours each month monitoring his credit, bank, and other account statements for evidence of identity theft and fraud, and anticipates continuing to do so for the foreseeable future.

51. **Plaintiff Mitchell Staggs** is a citizen and resident of the State of Iowa. Plaintiff Staggs created his Facebook account approximately nine years ago. Plaintiff Staggs maintains his Facebook account to the present day. Plaintiff Staggs has accessed his Facebook account from a mobile phone. Plaintiff Staggs has watched and "liked" videos on Facebook and has also "liked" pages on Facebook that contain videos. Plaintiff Staggs also uses Facebook messenger and/or instant messaging through Facebook. Plaintiff Staggs shared content and information with Facebook, which he expected Facebook to protect and secure against access by or disclosure to unauthorized parties. In approximately April 2018, Plaintiff Staggs received notice from Facebook that his content and information may have been obtained by the This Is Your Digital Life app, because one of Plaintiff Staggs's Facebook friends downloaded the This Is Your Digital Life app. Plaintiff Staggs was not aware of and did not consent to the sharing of his content and information with the This Is Your Digital Life app. Moreover, Plaintiff Staggs did not consent to any third-parties accessing his content and information through his Facebook friends and had no knowledge that Facebook had authorized this disclosure of his content and information without his consent.

52. During the 2016 U.S. Presidential election, Plaintiff Staggs frequently received political advertisements while using Facebook. On information and belief, Plaintiff Staggs was targeted by some or all of these advertisements as a result of the Cambridge Analytica Scandal. As a result of the release of his content and information, Plaintiff Staggs has suffered emotional distress, including anxiety, concern, and unease about unauthorized parties viewing and using his

content and information for improper purposes, such as identity theft and fraud as well as further intruding upon Plaintiff Staggs's private affairs and concerns, as detailed herein. Plaintiff Staggs fears that he is at risk of identity theft and fraud, and now spends approximately five to ten hours each month monitoring his credit, bank, and other account statements for evidence of identity theft and fraud, and anticipates continuing to do so for the foreseeable future.

53. **Plaintiff Dustin Short** is a citizen and resident of the State of Kansas. Plaintiff Short created his Facebook account approximately twelve years ago. Plaintiff Short maintains his Facebook account to the present day. Plaintiff Short has accessed his Facebook account from a mobile phone and a personal computer. Plaintiff Short has watched and "liked" videos on Facebook and has also "liked" pages on Facebook that contain videos. Plaintiff Short also uses Facebook messenger and/or instant messaging through Facebook. Plaintiff Short shared content and information with Facebook, which he expected Facebook to protect and secure against access by or disclosure to unauthorized parties. In approximately April 2018, Plaintiff Short received notice from Facebook that his content and information may have been obtained by the This Is Your Digital Life app, because one of Plaintiff Short's Facebook friends downloaded the This Is Your Digital Life app. Plaintiff Short was not aware of and did not consent to the sharing of his content and information with the This Is Your Digital Life app. Moreover, Plaintiff Short did not consent to any third-parties accessing his content and information through his Facebook friends and had no knowledge that Facebook had authorized this disclosure of his content and information without his consent.

54. During the 2016 U.S. Presidential election, Plaintiff Short frequently received political advertisements while using Facebook. On information and belief, Plaintiff Short was targeted by some or all of these advertisements as a result of the Cambridge Analytica Scandal. As a result of the release of his content and information, Plaintiff Short has suffered emotional distress, including anxiety, concern, and unease about unauthorized parties viewing and using his content and information for improper purposes, such as identity theft and fraud as well as further intruding upon Plaintiff Short's private affairs and concerns, as detailed herein. Plaintiff Short



fears that he is at risk of identity theft and fraud, and now spends approximately ten hours each month monitoring his credit, bank, and other account statements for evidence of identity theft and fraud, and anticipates continuing to do so for the foreseeable future. Because of his heightened risk of identity theft and fraud, Plaintiff Short has purchased credit monitoring and identity theft protection services, and anticipates continuing to pay for such services for the foreseeable future.

55. **Plaintiff Barbara Vance-Guerbe** is a citizen and resident of the State of Michigan. Plaintiff Vance-Guerbe created her Facebook account approximately eight years ago. Plaintiff Vance-Guerbe maintains her Facebook account to the present day. Plaintiff Vance-Guerbe has accessed her Facebook account from a mobile phone. Plaintiff Vance-Guerbe has watched and “liked” videos on Facebook and has also “liked” pages on Facebook that contain videos. Plaintiff Vance-Guerbe also uses Facebook messenger and/or instant messaging through Facebook. Plaintiff Vance-Guerbe shared content and information with Facebook, which she expected Facebook to protect and secure against access by or disclosure to unauthorized parties. Plaintiff Vance-Guerbe confirmed on Facebook that her content and information “was likely shared with” and may have been “misused” by the This Is Your Digital Life app, because one of Plaintiff Vance-Guerbe’s Facebook friends downloaded the This Is Your Digital Life app. Plaintiff Vance-Guerbe was not aware of and did not consent to the sharing of her content and information with the This Is Your Digital Life app. Moreover, Plaintiff Vance-Guerbe did not consent to any third-parties accessing her content and information through her Facebook friends and had no knowledge that Facebook had authorized this disclosure of her content and information without her consent.

56. During the 2016 U.S. Presidential election, Plaintiff Vance-Guerbe frequently received political advertisements while using Facebook. On information and belief, Plaintiff Vance-Guerbe was targeted by some or all of these advertisements as a result of the Cambridge Analytica Scandal. As a result of the release of her content and information, Plaintiff Vance-Guerbe has suffered emotional distress, including anxiety, concern, and unease about

unauthorized parties viewing and using her content and information for improper purposes, such as identity theft and fraud as well as further intruding upon Plaintiff Vance-Guerbe's private affairs and concerns, as detailed herein. Plaintiff Vance-Guerbe fears that she is at risk of identity theft and fraud.

57. **Plaintiff Jason Ariciu** is a citizen and resident of the State of Missouri. Plaintiff Ariciu created his Facebook account approximately thirteen years ago. Plaintiff Ariciu maintains his Facebook account to the present day. Plaintiff Ariciu has accessed his Facebook account from a mobile phone, a tablet, laptops, and personal computers. Plaintiff Ariciu has watched and "liked" videos on Facebook and has also "liked" pages on Facebook that contain videos. Plaintiff Ariciu also uses Facebook messenger. Plaintiff Ariciu shared content and information with Facebook, which he expected Facebook to protect and secure against access by or disclosure to unauthorized parties. Plaintiff Ariciu confirmed on Facebook that his content and information "was likely shared with" the This Is Your Digital Life app, because one of Plaintiff Ariciu's Facebook friends downloaded the This Is Your Digital Life app. Plaintiff Ariciu was not aware of and did not consent to the sharing of his content and information with the This Is Your Digital Life app. Moreover, Plaintiff Ariciu did not consent to any third-parties accessing his content and information through his Facebook friends and had no knowledge that Facebook had authorized this disclosure of his content and information without his consent.

58. During the 2016 U.S. Presidential election, Plaintiff Ariciu received political advertisements while using Facebook. On information and belief, Plaintiff Ariciu was targeted by some or all of these advertisements as a result of the Cambridge Analytica Scandal. As a result of the release of his content and information, Plaintiff Ariciu has suffered emotional distress, including anxiety, concern, and unease about unauthorized parties viewing and using his content and information for improper purposes, such as identity theft and fraud as well as further intruding upon Plaintiff Ariciu's private affairs and concerns, as detailed herein. Plaintiff Ariciu fears that he is at risk of identity theft and fraud, and now spends approximately four hours each

month monitoring his credit, bank, and other account statements for evidence of identity theft and fraud, and anticipates continuing to do so for the foreseeable future.

59. **Plaintiff William Lloyd** is a citizen and resident of the State of New York. Plaintiff Lloyd created his Facebook account approximately four and one-half years ago. Plaintiff Lloyd maintains his Facebook account to the present. Plaintiff Lloyd has accessed his Facebook account from a mobile phone and a personal computer. Plaintiff Lloyd has watched and “liked” videos on Facebook and has also “liked” pages on Facebook that contain videos. Plaintiff Lloyd also uses Facebook messenger and/or instant messaging through Facebook. Plaintiff Lloyd shared content and information with Facebook, which he expected Facebook to protect and secure against access by or disclosure to unauthorized parties. Plaintiff Lloyd confirmed on Facebook that his content and information “was likely shared with” and may have been “misused” by the This Is Your Digital Life app, because one of Plaintiff Lloyd’s Facebook friends downloaded the This Is Your Digital Life app. Plaintiff Lloyd was not aware of and did not consent to the sharing of his content and information with the This Is Your Digital Life app. Moreover, Plaintiff Lloyd did not consent to any third-parties accessing his content and information through his Facebook friends and had no knowledge that Facebook had authorized this disclosure of his content and information without his consent.

60. During the 2016 U.S. Presidential election, Plaintiff Lloyd frequently received political advertisements while using Facebook. On information and belief, Plaintiff Lloyd was targeted by some or all of these advertisements as a result of the Cambridge Analytica Scandal. As a result of the release of his content and information, Plaintiff Lloyd has suffered emotional distress, including anxiety, concern, and unease about unauthorized parties viewing and using his content and information for improper purposes, such as identity theft and fraud as well as further intruding upon Plaintiff Lloyd’s private affairs and concerns, as detailed herein. Plaintiff Lloyd fears that he is at risk of identity theft and fraud, and now spends approximately one hour each month monitoring his credit, bank, and other account statements for evidence of identity theft and fraud, and anticipates continuing to do so for the foreseeable future.

61. **Plaintiff Cheryl Senko** is a citizen and resident of the State of Ohio. Plaintiff Senko created her Facebook account approximately thirteen years ago. Plaintiff Senko maintains her Facebook account to the present day. Plaintiff Senko has accessed her Facebook account from mobile phones, laptops, personal computers, and a tablet. Plaintiff Senko has watched and “liked” videos on Facebook and has also “liked” pages on Facebook that contain videos. Plaintiff Senko also uses Facebook messenger. Plaintiff Senko shared content and information with Facebook, which she expected Facebook to protect and secure against access by or disclosure to unauthorized parties. Plaintiff Senko confirmed on Facebook that her content and information “was likely shared with” the This Is Your Digital Life app, because one of Plaintiff Senko’s Facebook friends downloaded the This Is Your Digital Life app. Plaintiff Senko was not aware of and did not consent to the sharing of her content and information with the This Is Your Digital Life app. Moreover, Plaintiff Senko did not consent to any third-parties accessing her content and information through her Facebook friends and had no knowledge that Facebook had authorized this disclosure of her content and information without her consent.

62. During the 2016 U.S. Presidential election, Plaintiff Senko frequently received political advertisements while using Facebook. On information and belief, Plaintiff Senko was targeted by some or all of these advertisements as a result of the Cambridge Analytica Scandal. As a result of the release of her content and information, Plaintiff Senko has suffered emotional distress, including anxiety, concern, and unease about unauthorized parties viewing and using her content and information for improper purposes, such as identity theft and fraud as well as further intruding upon Plaintiff Senko’s private affairs and concerns, as detailed herein. Plaintiff Senko fears that she is at risk of identity theft and fraud, and now spends approximately one hour each month monitoring her credit, bank, and other account statements for evidence of identity theft and fraud, and anticipates continuing to do so for the foreseeable future. Because of her heightened risk of identity theft and fraud, Plaintiff Senko enrolled in the credit monitoring service offered by her auto loan company.

63. **Plaintiff Ian Miller** is a citizen and resident of the State of Oklahoma. Plaintiff Miller created his Facebook account approximately twelve years ago. Plaintiff Miller maintains his Facebook account to the present day. Plaintiff Miller has accessed his Facebook account from a mobile phone and a personal computer. Plaintiff Miller has watched and “liked” videos on Facebook and has also “liked” pages on Facebook that contain videos. Plaintiff Miller also uses Facebook messenger and/or instant messaging through Facebook. Plaintiff Miller shared content and information with Facebook, which he expected Facebook to protect and secure against access by or disclosure to unauthorized parties. In approximately April 2018, Plaintiff Miller learned that millions of Facebook users’ content and information may have been obtained by the This Is Your Digital Life app, because Plaintiff Miller downloaded the This Is Your Digital Life app. Plaintiff Miller was not aware of and did not consent to the potential sharing of his content and information with the This Is Your Digital Life app. Moreover, Plaintiff Miller did not consent to any third-parties accessing his content and information through his Facebook friends and had no knowledge that Facebook had authorized this disclosure of his content and information without his consent.

64. As a result of this concern for the security of his content and information, Plaintiff Miller has suffered emotional distress, including anxiety, concern, and unease about unauthorized parties viewing and using his content and information for improper purposes, such as identity theft and fraud as well as further intruding upon Plaintiff Miller’s private affairs and concerns, as detailed herein. Plaintiff Miller fears that he is at risk of identity theft and fraud, and now spends approximately five hours each month monitoring his credit, bank, and other account statements for evidence of identity theft and fraud, and anticipates continuing to do so for the foreseeable future.

65. **Plaintiff James Tronka** is a citizen and a resident of the State of Pennsylvania. Plaintiff Tronka created his Facebook account approximately ten years ago. Plaintiff Tronka maintains his Facebook account to the present day. Plaintiff Tronka has accessed his Facebook account from a mobile phone. Plaintiff Tronka has watched and “liked” videos on Facebook and

has also “liked” pages on Facebook that contain videos. Plaintiff Tronka also uses Facebook messenger and/or instant messaging through Facebook. Plaintiff Tronka shared content and information with Facebook, which he expected Facebook to protect and secure against access by or disclosure to unauthorized parties. Plaintiff Tronka confirmed on Facebook that his content and information that his content and information may have been “shared” with and misused by the This Is Your Digital Life app, because one of Plaintiff Tronka’s Facebook friends downloaded the This Is Your Digital Life app. Plaintiff Tronka was not aware of and did not consent to the sharing of his content and information with the This Is Your Digital Life app. Moreover, Plaintiff Tronka did not consent to any third-parties accessing his content and information through his Facebook friends and had no knowledge that Facebook had authorized this disclosure of his content and information without his consent.

66. During the 2016 U.S. Presidential election, Plaintiff Tronka frequently received political advertisements while using Facebook. On information and belief, Plaintiff Tronka was targeted by some or all of these advertisements as a result of the Cambridge Analytica Scandal. As a result of the release of his content and information, Plaintiff Tronka has suffered emotional distress, including anxiety, concern, and unease about unauthorized parties viewing and using his content and information for improper purposes, such as identity theft and fraud as well as further intruding upon Plaintiff Tronka’s private affairs and concerns, as detailed herein. Plaintiff Tronka fears that he is at risk of identity theft and fraud, and now spends approximately two to three hours each month monitoring his credit, bank, and other account statements for evidence of identity theft and fraud, and anticipates continuing to do so for the foreseeable future.

67. **Plaintiff Steven Akins** is a citizen and resident of the State of Tennessee. Plaintiff Akins created his Facebook account approximately ten years ago. Plaintiff Akins maintains his Facebook account to the present day. Plaintiff Akins has accessed his Facebook account from mobile phones and personal computers. Plaintiff Akins has watched and “liked” videos on Facebook and has also “liked” pages on Facebook that contain videos. Plaintiff Akins also uses Facebook messenger and/or instant messaging through Facebook. Plaintiff Akins

shared content and information with Facebook, which he expected Facebook to protect and secure against access by or disclosure to unauthorized parties. On information and belief, Plaintiff Akins asserts his content and information was disclosed without his consent to the This Is Your Digital Life app or other third-party apps Facebook is investigating for misusing users' content and information. Plaintiff Akins was not aware of and did not consent to the sharing of his content and information with the This Is Your Digital Life app or other third parties. Moreover, Plaintiff Akins did not consent to any third-parties accessing his content and information through his Facebook friends and had no knowledge that Facebook had authorized this disclosure of his content and information without his consent.

68. During the 2016 U.S. Presidential election, Plaintiff Akins frequently received political advertisements while using Facebook. On information and belief, Plaintiff Akins was targeted by some or all of these advertisements as a result of the Cambridge Analytica Scandal. As a result of the release of his content and information, Plaintiff Akins has suffered emotional distress, including anxiety, concern, and unease about unauthorized parties viewing and using his content and information for improper purposes, such as identity theft and fraud as well as further intruding upon Plaintiff Akins's private affairs and concerns, as detailed herein. Plaintiff Akins fears that he is at risk of identity theft and fraud, and now spends approximately two hours each month monitoring his credit, bank, and other account statements for evidence of identity theft and fraud, and anticipates continuing to do so for the foreseeable future.

69. **Plaintiff Tyler King** is a citizen and resident of the State of Texas. Plaintiff King created her Facebook account approximately ten years ago. Upon learning of the Cambridge Analytica Scandal, Plaintiff King deleted her Facebook account. Plaintiff King accessed her Facebook account from a mobile phone, a tablet, a laptop, and a personal computer. Plaintiff King watched and "liked" videos on Facebook and also "liked" pages on Facebook that contained videos. Plaintiff King also used Facebook messenger. Plaintiff King shared content and information with Facebook, which she expected Facebook to protect and secure against access by or disclosure to unauthorized parties. Plaintiff King confirmed on Facebook that her

content and information “was likely shared with” and may have been “misused” by the This Is Your Digital Life app. Plaintiff King was not aware of and did not consent to the sharing of her content and information with the This Is Your Digital Life app. Moreover, Plaintiff King did not consent to any third-parties accessing her content and information through her Facebook friends and had no knowledge that Facebook had authorized this disclosure of her content and information without her consent.

70. During the 2016 U.S. Presidential election, Plaintiff King frequently received political advertisements while using Facebook. On information and belief, Plaintiff King was targeted by some or all of these advertisements as a result of the Cambridge Analytica Scandal. As a result of the release of her content and information, Plaintiff King has suffered emotional distress, including anxiety, concern, and unease about unauthorized parties viewing and using her content and information for improper purposes, such as identity theft and fraud as well as further intruding upon Plaintiff King’s private affairs and concerns, as detailed herein. Plaintiff King fears that she is at risk of identity theft and fraud, and now spends approximately one hour each month monitoring her credit, bank, and other account statements for evidence of identity theft and fraud, and anticipates continuing to do so for the foreseeable future.

71. **Plaintiff Gretchen Maxwell** is a citizen and resident of the State of Texas. Plaintiff Maxwell created her Facebook account approximately nine years ago. Upon learning of the Cambridge Analytica Scandal, Plaintiff Maxwell deactivated her Facebook account. Plaintiff Maxwell accessed her Facebook account from a mobile phone, a tablet, and a personal computer. Plaintiff Maxwell watched and “liked” videos on Facebook and also “liked” pages on Facebook that contained videos. Plaintiff Maxwell also used Facebook messenger. Plaintiff Maxwell shared content and information with Facebook, which she expected Facebook to protect and secure against access by or disclosure to unauthorized parties. Plaintiff Maxwell confirmed on Facebook that her content and information may have been “shared” with and “misused” by the This Is Your Digital Life app, because one of Plaintiff Maxwell’s Facebook friends downloaded the This Is Your Digital Life app. Plaintiff Maxwell was not aware of and did not consent to the



sharing of her content and information with the This Is Your Digital Life app. Moreover, Plaintiff Maxwell did not consent to any third-parties accessing her content and information through her Facebook friends and had no knowledge that Facebook had authorized this disclosure of her content and information without her consent.

72. As a result of the release of her content and information, Plaintiff Maxwell has suffered emotional distress, including anxiety, concern, and unease about unauthorized parties viewing and using her content and information for improper purposes, such as identity theft and fraud as well as further intruding upon Plaintiff Maxwell's private affairs and concerns, as detailed herein.

73. **Plaintiff Scott Schinder** is a citizen and resident of the State of Texas. Plaintiff Schinder created his Facebook account approximately eleven years ago. Plaintiff Schinder maintains his Facebook account to the present day. Plaintiff Schinder has accessed his Facebook account from a mobile phone and a personal computer. Plaintiff Schinder has watched and "liked" videos on Facebook and has also "liked" pages on Facebook that contain videos. Plaintiff Schinder also uses Facebook messenger and/or instant messaging through Facebook. Plaintiff Schinder shared content and information with Facebook, which he expected Facebook to protect and secure against access by or disclosure to unauthorized parties. In approximately April 2018, Plaintiff Schinder received notice from Facebook that his content and information may have been obtained by the This Is Your Digital Life app, because one of Plaintiff Schinder's Facebook friends downloaded the This Is Your Digital Life app. Plaintiff Schinder was not aware of and did not consent to the sharing of his content and information with the This Is Your Digital Life app. Moreover, Plaintiff Schinder did not consent to any third-parties accessing his content and information through his Facebook friends and had no knowledge that Facebook had authorized this disclosure of his content and information without his consent.

74. During the 2016 U.S. Presidential election, Plaintiff Schinder frequently received political advertisements while using Facebook. On information and belief, Plaintiff Schinder was targeted by some or all of these advertisements as a result of the Cambridge Analytica Scandal.

As a result of the release of his content and information, Plaintiff Schinder has suffered emotional distress, including anxiety, concern, and unease about unauthorized parties viewing and using his content and information for improper purposes, such as identity theft and fraud as well as further intruding upon Plaintiff Schinder's private affairs and concerns, as detailed herein. Plaintiff Schinder fears that he is at risk of identity theft and fraud, and now spends approximately eight hours each month monitoring his credit, bank, and other account statements for evidence of identity theft and fraud, and anticipates continuing to do so for the foreseeable future.

75. **Plaintiff Mary Beth Grisi** is a citizen and resident of the State of Virginia. Plaintiff Grisi created her Facebook account approximately nine years ago. Plaintiff Grisi maintains her Facebook account to the present day. Plaintiff Grisi accessed her Facebook account from a mobile phone and a personal computer. Plaintiff Grisi watched and "liked" videos on Facebook and also "liked" pages on Facebook that contained videos. Plaintiff Grisi also used Facebook messenger and/or instant messaging through Facebook. Plaintiff Grisi shared content and information with Facebook, which she expected Facebook to protect and secure against access by or disclosure to unauthorized parties. Plaintiff Grisi confirmed on Facebook that her content and information "was likely shared with" the This Is Your Digital Life app, because one of Plaintiff Grisi's Facebook friends downloaded the This Is Your Digital Life app. Plaintiff Grisi was not aware of and did not consent to the sharing of her content and information with the This Is Your Digital Life app. Moreover, Plaintiff Grisi did not consent to any third-parties accessing her content and information through her Facebook friends and had no knowledge that Facebook had authorized this disclosure of her content and information without her consent.

76. As a result of the release of her content and information, Plaintiff Grisi has suffered emotional distress, including anxiety, concern, and unease about unauthorized parties viewing and using her content and information for improper purposes, such as identity theft and fraud as well as further intruding upon Plaintiff Grisi's private affairs and concerns, as detailed

herein. Plaintiff Grisi fears that she is at risk of identity theft and fraud, and now spends approximately seven hours each month monitoring her credit, bank, and other account statements for evidence of identity theft and fraud, and anticipates continuing to do so for the foreseeable future. Because of her heightened risk of identity theft and fraud, Plaintiff Grisi enrolled in the credit monitoring service offered by her credit card company.

77. **Plaintiff Suzie Haslinger** is a citizen and resident of the State of Virginia. Plaintiff Haslinger created her Facebook account approximately nine years ago. Plaintiff Haslinger maintains her Facebook account to the present day. Plaintiff Haslinger accessed her Facebook account from a mobile phone. Plaintiff Haslinger watched and “liked” videos on Facebook and also “liked” pages on Facebook that contained videos. Plaintiff Haslinger also used Facebook messenger and/or instant messaging through Facebook. Plaintiff Haslinger shared content and information with Facebook, which she expected Facebook to protect and secure against access by or disclosure to unauthorized parties. On information and belief, Plaintiff Haslinger asserts her content and information was disclosed without her consent to the This Is Your Digital Life app or other third-party apps Facebook is investigating for misusing users’ content and information. Plaintiff Haslinger was not aware of and did not consent to the sharing of her content and information with the This Is Your Digital Life app or other third parties. Moreover, Plaintiff Haslinger did not consent to any third-parties accessing her content and information through her Facebook friends and had no knowledge that Facebook had authorized this disclosure of her content and information without her consent.

78. As a result of the release of her content and information, Plaintiff Haslinger has suffered emotional distress, including anxiety, concern, and unease about unauthorized parties viewing and using her content and information for improper purposes, such as identity theft and fraud as well as further intruding upon Plaintiff Haslinger’s private affairs and concerns, as detailed herein. Plaintiff Haslinger fears that she is at risk of identity theft and fraud, and now spends approximately twelve hours each month monitoring her credit, bank, and other account

statements for evidence of identity theft and fraud, and anticipates continuing to do so for the foreseeable future.

79. **Plaintiff Terry Fischer** is a citizen and resident of the State of Washington. Plaintiff Fischer created her Facebook account approximately five years ago. Plaintiff Fischer maintains her Facebook account to the present day. Plaintiff Fischer accessed her Facebook account from a mobile phone and a personal computer. Plaintiff Fischer watched and “liked” videos on Facebook and also “liked” pages on Facebook that contained videos. Plaintiff Fischer also used Facebook messenger. Plaintiff Fischer shared content and information with Facebook, which she expected Facebook to protect and secure against access by or disclosure to unauthorized parties. Plaintiff Fischer confirmed on Facebook that her content and information “was likely shared” with and may have been “misused” by the This Is Your Digital Life app, because Plaintiff Fischer downloaded and logged into the This Is Your Digital Life app. Plaintiff Fischer was not aware of and did not consent to the sharing of her content and information with the This Is Your Digital Life app. Moreover, Plaintiff Fischer did not consent to any third-parties accessing her content and information through her Facebook friends and had no knowledge that Facebook had authorized this disclosure of her content and information without her consent.

80. As a result of the release of her content and information, Plaintiff Fischer has suffered emotional distress, including anxiety, concern, and unease about unauthorized parties viewing and using her content and information for improper purposes, such as identity theft and fraud as well as further intruding upon Plaintiff Fischer’s private affairs and concerns, as detailed herein. Plaintiff Fischer fears that she is at risk of identity theft and fraud, and now spends approximately two to three hours each month monitoring her credit, bank, and other account statements for evidence of identity theft and fraud, and anticipates continuing to do so for the foreseeable future. Because of her heightened risk of identity theft and fraud, Plaintiff Fischer has frozen and requested fraud alerts from the various credit monitoring agencies and anticipates continuing to utilize such services for the foreseeable future.

81. **Plaintiff Taunna Jarvimaki** is a citizen and resident of the State of Washington. Plaintiff Jarvimaki created her Facebook account approximately nine years ago. Plaintiff Jarvimaki maintains her Facebook account to the present day. Plaintiff Jarvimaki accessed her Facebook account from a mobile phone, a laptop, and a personal computer. Plaintiff Jarvimaki watched and “liked” videos on Facebook and also “liked” pages on Facebook that contained videos. Plaintiff Jarvimaki also used Facebook messenger and/or instant messaging through Facebook. Plaintiff Jarvimaki shared content and information with Facebook, which she expected Facebook to protect and secure against access by or disclosure to unauthorized parties. Plaintiff Jarvimaki confirmed on Facebook that her content and information may have been “shared” with and “may have been misused” by the This Is Your Digital Life app, because one of Plaintiff Jarvimaki’s Facebook friends downloaded the This Is Your Digital Life app. Plaintiff Jarvimaki was not aware of and did not consent to the sharing of her content and information with the This Is Your Digital Life app. Moreover, Plaintiff Jarvimaki did not consent to any third-parties accessing her content and information through her Facebook friends and had no knowledge that Facebook had authorized this disclosure of her content and information without her consent.

82. As a result of the release of her content and information, Plaintiff Jarvimaki has suffered emotional distress, including anxiety, concern, and unease about unauthorized parties viewing and using her content and information for improper purposes, such as identity theft and fraud as well as further intruding upon Plaintiff Jarvimaki’s private affairs and concerns, as detailed herein. Plaintiff Jarvimaki fears that she is at risk of identity theft and fraud, and now spends approximately thirty minutes each month monitoring her credit, bank, and other account statements for evidence of identity theft and fraud, and anticipates continuing to do so for the foreseeable future. Because of her heightened risk of identity theft and fraud, Plaintiff Jarvimaki enrolled in various credit monitoring services offered to her.

83. **Plaintiff Sandra Adkins** is a citizen and a resident of the State of West Virginia. Plaintiff Adkins created her Facebook account approximately ten years ago. Plaintiff Adkins

maintains her Facebook account to the present day. Plaintiff Adkins has accessed her Facebook account from a mobile phone. Plaintiff Adkins has watched and “liked” videos on Facebook and has also “liked” pages on Facebook that contain videos. Plaintiff Adkins also uses Facebook messenger and/or instant messaging through Facebook. Plaintiff Adkins shared content and information with Facebook, which she expected Facebook to protect and secure against access by or disclosure to unauthorized parties. Plaintiff Adkins confirmed on Facebook that her content and information may have been “shared” with and “misused” by the This Is Your Digital Life app, because one of Plaintiff Adkins’ Facebook friends downloaded the This Is Your Digital Life app. Plaintiff Adkins was not aware of and did not consent to the sharing of her content and information with the This Is Your Digital Life app. Moreover, Plaintiff Adkins did not consent to any third-parties accessing her content and information through her Facebook friends and had no knowledge that Facebook had authorized this disclosure of her content and information without her consent.

84. During the 2016 U.S. Presidential election, Plaintiff Adkins frequently received political advertisements while using Facebook. On information and belief, Plaintiff Adkins was targeted by some or all of these advertisements as a result of the Cambridge Analytica Scandal. As a result of the release of her content and information, Plaintiff Adkins has suffered emotional distress, including anxiety, concern, and unease about unauthorized parties viewing and using her content and information for improper purposes, such as identity theft and fraud as well as further intruding upon Plaintiff Adkins’ private affairs and concerns, as detailed herein. Plaintiff Adkins fears that she is at risk of identity theft and fraud, and now spends approximately one hour each month monitoring her credit, bank, and other account statements for evidence of identity theft and fraud, and anticipates continuing to do so for the foreseeable future.

85. **Plaintiff Ashley Kmiecik** is a citizen and resident of the State of Wisconsin. Plaintiff Kmiecik created her Facebook account approximately five years ago. Plaintiff Kmiecik maintains her Facebook account to the present day. Plaintiff Kmiecik accessed her Facebook account from a mobile phone, a tablet, a laptop, and a personal computer. Plaintiff

Kmieciak watched and “liked” videos on Facebook and also “liked” pages on Facebook that contained videos. Plaintiff Kmiecik also used Facebook messenger and/or instant messaging through Facebook. Plaintiff Kmiecik shared content and information with Facebook, which she expected Facebook to protect and secure against access by or disclosure to unauthorized parties. Plaintiff Kmiecik confirmed on Facebook that her content and information may have been “shared” with and “misused” by the This Is Your Digital Life app, because one of Plaintiff Kmiecik’s Facebook friends downloaded the This Is Your Digital Life app. Plaintiff Kmiecik was not aware of and did not consent to the sharing of her content and information with the This Is Your Digital Life app. Moreover, Plaintiff Kmiecik did not consent to any third-parties accessing her content and information through her Facebook friends and had no knowledge that Facebook had authorized this disclosure of her content and information without her consent.

86. During the 2016 U.S. Presidential election, Plaintiff Kmiecik frequently received political advertisements while using Facebook. On information and belief, Plaintiff Kmiecik was targeted by some or all of these advertisements as a result of the Cambridge Analytica Scandal. As a result of the release of her content and information, Plaintiff Kmiecik has suffered emotional distress, including anxiety, concern, and unease about unauthorized parties viewing and using her content and information for improper purposes, such as identity theft and fraud as well as further intruding upon Plaintiff Kmiecik’s private affairs and concerns, as detailed herein. Plaintiff Kmiecik fears that she is at risk of identity theft and fraud, and now spends approximately two hours each month monitoring her credit, bank, and other account statements for evidence of identity theft and fraud, and anticipates continuing to do so for the foreseeable future.

87. **Plaintiff Bridget Peters** is a citizen and a resident of Hampshire, England in the United Kingdom. Plaintiff Peters created her Facebook account approximately ten years ago. Plaintiff Peters maintains her Facebook account to the present day. Plaintiff Peters has accessed her Facebook account from a mobile phone and a personal computer. Plaintiff Peters has watched and “liked” videos on Facebook and has also “liked” pages on Facebook that contain

videos. Plaintiff Peters also uses Facebook messenger and/or instant messaging through Facebook. Plaintiff Peters shared content and information with Facebook, which she expected Facebook to protect and secure against access by or disclosure to unauthorized parties. On information and belief, Plaintiff Peters asserts her content and information was disclosed without her consent to the This Is Your Digital Life app or other third-party apps Facebook is investigating for misusing users' content and information. Plaintiff Peters was not aware of and did not consent to the sharing of her content and information with the This Is Your Digital Life app. Moreover, Plaintiff Peters did not consent to any third-parties accessing her content and information through her Facebook friends and had no knowledge that Facebook had authorized this disclosure of her content and information without her consent.

88. As a result of the release of her content and information, Plaintiff Peters has suffered emotional distress, including anxiety, concern, and unease about unauthorized parties viewing and using her content and information for improper purposes, such as identity theft and fraud as well as further intruding upon Plaintiff Peters' private affairs and concerns, as detailed herein. Plaintiff Peters fears that she is at risk of identity theft and fraud, and now spends approximately one hour each month monitoring her credit, bank, and other account statements for evidence of identity theft and fraud, and anticipates continuing to do so for the foreseeable future.

## **B. Defendants and Co-Conspirators**

### **1. Prioritized Defendant and Doe Defendants:**

89. **Facebook, Inc.** ("Facebook"), a publicly traded company, is incorporated in the State of Delaware, with its executive offices located at 1601 Willow Road, Menlo Park, California 94025 and its headquarters located at 1 Hacker Way, Menlo Park, California 94025. Facebook is an online social media and social networking service company founded in 2004. In 2004 Facebook started as a social networking website enabling users to connect, share, and communicate with each other through text, photographs, and videos as well as to interact with third party apps such as games and quizzes on mobile devices and personal computers. Over



time, Facebook has evolved into its own platform that allows users to connect with each other while also acting as a data broker, harvesting user content and information and selling access to the data via targeted messaging to third parties such as advertisers, political action groups and others. Facebook's market value is currently estimated at more than \$473 billion, with annual revenues of \$40 billion from advertising.

90. **Doe Defendants 1-100:** Plaintiffs do not know the true names of Doe Defendants 1-100, inclusive, and therefore sue them by those fictitious names. Plaintiffs are informed and believe, and on the basis of that information and belief, allege that each of those defendants were proximately responsible for the events and happenings alleged in this Complaint and for Plaintiffs' injuries and damages.

**2. Non-Prioritized Defendants (Individual Defendants Named in Actions Consolidated in this MDL As to Whom Co-Lead Counsel Seek a Stay)**

91. **Stephen Kevin Bannon** is a resident of the District of Columbia. At all relevant times, Bannon was a part owner, Vice President, and Secretary of Cambridge Analytica until he resigned from those positions to act as the chief executive of Donald Trump's presidential campaign. At all relevant times, Bannon had decision-making authority at Cambridge Analytica and directed and approved the actions taken by Cambridge Analytica alleged herein.

92. **Aleksandr Kogan**, a/k/a Aleksandr Spectre, is a resident of the state of California and Cambridge, England. Dr. Kogan was a founder of GSR. At all relevant times, Dr. Kogan had decision-making authority at GSR and directed, approved, or otherwise ratified the actions taken by GSR as alleged herein.

93. **Robert Leroy Mercer** is an individual resident of New York, New York. Mercer, an American hedge-fund manager, reportedly invested millions of dollars in Cambridge Analytica, and Rebekah Mercer (Mercer's daughter) sits on Cambridge Analytica's Board of Directors. the *Guardian* reported that Mercer met with Cambridge Analytica's CEO Alexander Nix and Christopher Wylie in New York, New York to discuss the plan to harvest and use

Facebook users' data in order to create sophisticated psychological and political profiles.<sup>4</sup> Wylie told the *Guardian* about that meeting, stating Mercer "said very little, but he really listened. He wanted to understand the science. And he wanted proof that it worked."<sup>5</sup>

94. **Sheryl Kara Sandberg** is an individual residing in Menlo Park, California. Ms. Sandberg is the chief operating officer ("COO") of Facebook. Ms. Sandberg has served as Facebook's COO since 2008, and has been a member of Facebook's Board since 2012. As Facebook's COO, Ms. Sandberg is responsible for Facebook's day-to-day operations and reports directly to Defendant Zuckerberg. Ms. Sandberg oversees Facebook's business operations, including sales, marketing, business development, human resources, public policy, and communications. Ms. Sandberg was instrumental in developing Facebook's online advertising programs, and was the "architect" of Facebook's transformation "into a global advertising juggernaut."

95. **Mark Elliot Zuckerberg** is an individual residing in Palo Alto, California. Mr. Zuckerberg is the founder of Facebook and has served as Facebook's CEO and as a member of the Board since July 2004, and as Chairman of the Board since January 2012. Mr. Zuckerberg is responsible for Facebook's day-to-day operations, as well as the overall direction and product strategy of Facebook. He is also Facebook's controlling stockholder with ownership of stock and proxies for stock representing more than 53.3% of Facebook's voting power as of April 13, 2018, though he owns only 16% of Facebook's total equity.

#### C. **Unnamed Co-Conspirators: Cambridge-Analytica-Related Entities<sup>6</sup>**

96. **Cambridge Analytica LLC** ("Cambridge Analytica") is a privately held limited

---

<sup>4</sup> Carole Cadwalladr, *The Cambridge Analytica Files 'I Made Steve Bannon's Psychological Warfare Tool': Meet the Data War Whistleblower*, *Guardian* (Mar. 18, 2018), <https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wyliefacebook-nix-bannon-trump>.

<sup>5</sup> *Id.*

<sup>6</sup> These entities were named in prior complaints consolidated into this docket. These entities are not named here pursuant to Title 11, § 362 of the United States Bankruptcy Code in addition to this court's order staying claims. *See* Pretrial Order No. 5: Scheduling at 1, ECF No. 103 ("The

liability company organized under the laws of the State of Delaware, incorporated on December 31, 2013, with its principal offices located at 597 5th Avenue, 7th Floor, New York, New York 10017. Cambridge Analytica does business throughout the United States, including in this District. Cambridge Analytica maintains offices in London, New York, and Washington, D.C. Its registered agent for service of summons is The Corporation Trust Company, 1209 Orange Street, Corporation Trust Center, Wilmington, Delaware 19801. Cambridge Analytica is a political consulting and “behavioral microtargeting” firm that combines data mining, data brokerage, and data analysis with strategic communication for the electoral process. It was founded in 2013 as a subsidiary of its parent company SCL Group, to participate in American politics. In 2014, Cambridge Analytica was involved in 44 U.S. political races. Cambridge Analytica was also active in the Brexit campaign. According to the *Business Insider*, Defendant Stephen Bannon was Vice President of Cambridge Analytica from June 2014 until August 2016.

97. **Cambridge Analytica Commercial LLC** (“CA Commercial”) is a privately held limited liability company organized under the laws of the State of Delaware, incorporated on January 21, 2015, and is a division of Cambridge Analytica. CA Commercial’s registered agent for service of summons is The Corporation Trust Company, 1209 Orange Street, Corporation Trust Center, Wilmington, Delaware 19801. Cambridge Analytica is owned in part (19%) by SCL Elections Ltd, a British company owned by SCL Analytics Limited, which is owned in part by SCL Group. During the relevant time, Alexander Nix was CEO of both SCL Elections Ltd and Cambridge Analytica UK.

98. **Cambridge Analytica Holdings LLC** is a privately held limited liability company organized under the laws of the State of Delaware, incorporated on May 9, 2014. Cambridge Analytica Holdings, LLC’s registered agent for service of summons is The Corporation Trust Company, 1209 Orange Street, Corporation Trust Center, Wilmington, Delaware 19801. According to the *Guardian*, hedge fund billionaire Robert Mercer funded CA

---

case is stayed as to the Cambridge Analytica defendants pending the outcome of the parties’ request of the bankruptcy court for relief from the automatic stay.”).

Holdings, which created and initially ran Cambridge Analytica.<sup>7</sup>

99. **Cambridge Analytica Limited** is a British-registered company headquartered in London, England with U.S. offices located in New York, New York and Washington, D.C.

100. **Cambridge Analytica (UK) Limited** is a British-registered company headquartered in London, England with U.S. offices located in New York, New York and Washington, D.C. Prior to changing its name, Cambridge Analytica (UK) Limited was formerly registered as SCL USA Limited.

101. **Cambridge Analytica Political LLC** (“CA Political”) is a privately held limited liability company organized under the laws of the State of Delaware, incorporated on January 21, 2015, and is a division of Cambridge Analytica. CA Political’s registered agent for service of summons is The Corporation Trust Company, 1209 Orange Street, Corporation Trust Center, Wilmington, Delaware 19801.

102. Cambridge Analytica, CA Political and CA Commercial all share the same website: <https://cambridgeanalytica.org>. According to Cambridge Analytica’s website, CA Political and CA Commercial are Divisions of Cambridge Analytica LLC. Upon information and belief, CA Holdings is a shell holding company for shares of Cambridge Analytica, CA Political and CA Commercial.

103. **SCL Elections Limited** is a British company incorporated on October 17, 2012. Its address is listed as c/o PFK Littlejohn, chartered accountants located at 1 Westferry Circus, Canary Wharf, London, E14 4HD, United Kingdom. Alexander Nix is listed as a director of SCL Elections and the ultimate controlling party as of the end of 2015.

104. **SCL Group Limited**, formerly known as Strategic Communications Laboratories Ltd, is a British company registered with the UK Companies House in 2005. Its headquarters are located at 55 New Oxford Street, London, WC1A 1BS. SCL Group Limited also has multiple

---

<sup>7</sup> Carole Cadwalladr & Emma Graham-Harrison, *Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach*, Guardian (Mar. 17, 2018), <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>.

U.S. affiliates, including SCL Group Inc. with offices in New York located at 597 5th Avenue, 7th Floor, New York, New York, 10036, and SCL USA Inc. with offices in Washington, D.C. located at 1901 Pennsylvania Avenue, N.W., Washington, D.C. 20006.

105. **SCL USA Inc.** is a privately held company incorporated under the laws of the State of Delaware, incorporated on April 22, 2104, and is a wholly owned subsidiary of SCL Elections. Its address is 597 5th Avenue, 7th Floor, New York, New York 10017 and its registered agent for service of summons is Erisedentagent, Inc., 1013 Centre Road, Suite 403S, Wilmington, Delaware 19805. Alexander Nix is SCL USA Inc.'s CEO. SCL USA is the alter ego of SCL Group.

**D. Other Non-Defendant Co-Conspirator**

106. **Global Science Research Limited** was a United Kingdom company that harvested and sold the private information of social media users for profit. On information and belief, Global Science Research Limited ("GSR") did significant business in California, but has since dissolved. Its successors in interest are unknown at this time.

**IV. FACTUAL BACKGROUND**

**A. Facebook's Transition from Social Media Company to Data Broker**

107. Before the Cambridge Analytica Scandal, Facebook was generally understood to be a social media platform—a place where users voluntarily shared information about their personal lives with people whose "friends" status was mutually accepted. But as the public is only beginning to understand, Facebook is far more than a place to share information with a small subset of Facebook users—it is a repository for personal content and information about anyone who has used the internet, regardless of whether they use Facebook or not. The aggregation of this data with other available information makes it possible to de-anonymize the data that Facebook collects, and target people by name and any variety of assumed characteristics. In some sense, there is no escaping the data that is collected about you.

108. Facebook started as a user-driven experience. Users initially were comfortable sharing information about themselves on the social media platform in part because they believed

they controlled how their content and information was shared. Facebook recognizes this in its mission statement: “People use Facebook to stay connected with friends and family, to discover what’s going on in the world, and to share and express what matters to them.”

109. However, Facebook’s disastrous initial public offering (“IPO”) encouraged Facebook to focus on a business model that faced advertisers, not its users. Following its IPO, which, at the time, was the biggest Internet- based technology IPO in history, Facebook’s share price plummeted. From this experience, Facebook concluded that its initial “social networking” business model needed to change, and quickly, if the Company were to survive. Capitalizing upon the resources in the user data that it stored, in 2012, Facebook became a full-fledged data broker. First, the Company turned “likes” into product endorsements; next, it launched a marketplace for content and information about the people on its platform. But the most successful attempt to monetize data was through targeted marketing.<sup>8</sup> As the *Atlantic Monthly* expressed it at the time: “In 2012 Facebook launched over a dozen new initiatives to make money off of you—you being its product, of course.”<sup>9</sup> Facebook’s ability to sell targeted messaging to Facebook’s user population now drives its revenues and thus its share price.<sup>10</sup>

110. There is nothing wrong with targeted advertising. However, Facebook’s failure to apprise users of the extent to which it was sharing access to users’ content and information with business partners, in combination with Facebook’s failure to exert controls over that data once third parties accessed it, deprived those users of the choice to make informed decisions about what they were sharing. Users did not understand the extent to which their content was harvested or how it was being aggregated. As the architect of an entire system engineered to collect and sell access to that content, Facebook owed its users full disclosure. As *Wired* has expressed it: “One minute you’re filling out an app survey; the next, your answers are informing

---

<sup>8</sup> Rebecca Greenfield, *2012: The Year Facebook Finally Tried to Make Some Money*, Atlantic (Dec. 14, 2012), <https://www.theatlantic.com/technology/archive/2012/12/2012-year-facebook-finally-tried-make-some-money/320493/>.

<sup>9</sup> *Id.*

<sup>10</sup> Phil Simon, *Facebook: The New King of Data Brokers*, *Wired* (Oct. 1, 2014), <https://www.wired.com/insights/2014/10/facebook-king-data-brokers/>.

the psychographically targeted ads of a political campaign. No one signed up for that.”<sup>11</sup>

**B. Facebook Enables Apps, Websites, and Devices to Access Facebook Users’ Content and Information**

111. Facebook’s partnerships with third parties, including device makers and its app developers, have formed a large part of its data-brokerage strategy.

112. These partnerships allow Facebook to pool and aggregate information about billions of people for the purpose of targeting them with content. By engaging in partnerships with third party app developers, mobile devices makers, software makers, security firms, and even the chip designer Qualcomm, Facebook leveraged its position as a curator of user content and information.<sup>12</sup>

113. Facebook engineered application programming interfaces (“APIs”) to facilitate the collection of data for app developers and for its “business partners” like Apple, Samsung, Amazon and other third parties. An API is defined as a set of programming instructions and standards for accessing a Web-based software application or Web tool. An API can be thought of as the messenger between a system—be it a website, application, or, as here, Facebook—and someone wanting to access that system.

**1. How Facebook Enabled Third Parties to Gather and Disseminate Users’ Content and Information**

114. Facebook engineered a number of APIs available for app developers, device makers, and other business partners to use on Facebook. For example, an “Events API” allows users to grant an app permission to get information about events they host or attend, including private events. Facebook Events also provides information about other people’s attendance as well as posts on the event wall. Additionally, app developers may use a “Groups API” to make it easier for users to post and respond to content in their groups. There is also a “Pages API” which can be used to read posts or comments from any Page. Facebook reports that this helps

---

<sup>11</sup> Brian Barrett, *Facebook Owes You More Than This*, Wired (Mar. 19, 2018), <https://www.wired.com/story/facebook-privacy-transparency-cambridge-analytica/>.

<sup>12</sup> Natasha Lomas, *Facebook Gives US Lawmakers the Names of 52 Firms it Gave Deep Data Access to*, TechCrunch (July 2, 2018), <https://techcrunch.com/2018/07/02/facebook-gives-us-lawmakers-the-names-of-52-firms-it-gave-deep-data-access-to/>.

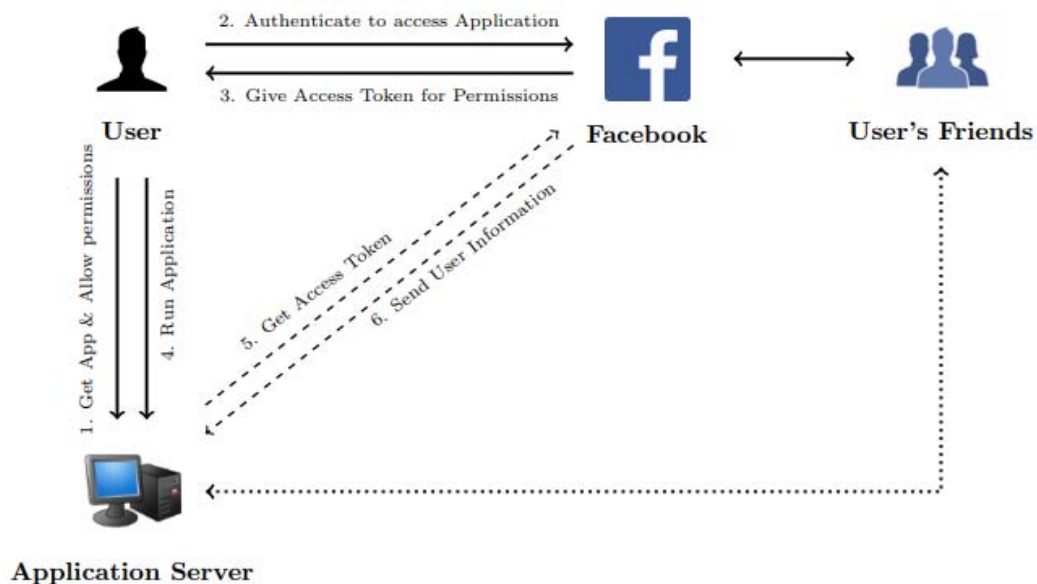


developers create tools for Page owners to help them do things like schedule posts and reply to comments or messages.

115. In April 2018, following the Cambridge Analytica Scandal and resulting inquiries, Facebook acknowledged that all three of these APIs could provide access to a great deal of data and thus decided to impose more requirements for app developers before they could gain access to user data through any of these APIs. The first API that Facebook developed, however, was very permissive. It was ultimately through this platform that Cambridge Analytica purchased the data of as many as 87 million Facebook users.

116. This first API was announced in April 2010 at Facebook’s annual developer conference. In unveiling this first API—called Open Graph API version 1.0, or “Graph API v.1.0”—Mr. Zuckerberg laid out his plan to turn the Web into what he called “instantly social experiences.”

117. To access Facebook data through Graph API v.1.0, developers needed to gain access through an “access token.” Access tokens allow data to be transmitted securely.



118. Graph API v.1.0 allowed external developers to reach out to Facebook users and request access a large chunk of their personal data—and, crucially, to access their Facebook



friends' personal data too. Users who joined before 2010 were not specifically or directly notified of this change.

119. This made a large swath of sensitive user content and information available to app developers. Graph API v.1.0 enabled app developers to access the app user's name, gender, birthdate, location, photos, and Page likes. And app developers could collect this information not just from the app user himself—depending on what that user's *friends* had chosen to share with him, developers could access this same information from those friends. Device makers and business partners had similar access.

120. There are two ways in which Facebook apps using the API v1 could access user-data: server-based and browser-based.

121. The server-based method works as follows: a user installs the app, which then allows the app to get an “access token” from Facebook. An access token is like a temporary user-specific password that enables the app to act on behalf of a user who has installed the app. Once the app receives an access token, it may use it to issue a request for certain user data (or friend data) to Facebook's server. As long as the request complies with the user's and/or friends' privacy settings, Facebook will respond to it by transmitting the requested data to the app server. The data contained in Facebook's response is then received and stored by the app server.

122. The browser-based method is slightly different. A user installs the app, which then resides in the user's web browser. After installation, the app obtains an “access token,” which is like a temporary user-specific password that enables the app to act on behalf of a user who has installed the app. While the user is using the app, the app, using the access token, may issue a request for certain user data (or friend data) to Facebook's server. As long as the request complies with the user's and/or friends' privacy settings, Facebook will respond to it by transmitting the requested data to the user's browser. The app sends this data from the user's browser to the app server, which stores it.

123. In the browser-based method, Facebook's server sends data to the user's browser. Unknown to Facebook or the user, the app code, which resides in the user's browser, captures

this data before it reaches the user and sends it to its own server. Thus, it is plausible to consider it an interception. In the server-based method, on the other hand, Facebook's server sends data to the app's server, so that an app residing in the user's browser cannot intercept it. Under Graph API v.1.0, app developers could access three kinds of information, depending on a users' settings and the app developers' permissions. These were (1) Basic Info (2) Extended Profile Properties, which are explained below; and (3) Extended Permissions. Each of these categories allowed third parties to access specific information. The graph below displays all categories of information available under Graph API v.1.0:

Basic Info (default)	Extended Profile Properties (xpP)		Extended Permissions (xP)
	User Data	Friends Data	
uid	user_about_me	friends_about_me	ads_management
name	user_actions.books	friends_actions.books	ads_read
first_name	user_actions.music	friends_actions.music	create_event
last_name	user_actions.news	friends_actions.news	create_note
link	user_actions.video	friends_actions.video	email
username	user_activities	friends_activities	export_stream
gender	user_birthday	friends_birthday	manage_friendlists
locale	user_checkins	friends_checkins	manage_notifications
age-range	user_education.history	friends_education.history	manage_pages
	user_events	friends_events	photo_upload
	user_friends	friends_games.activity	publish_actions
	user_games.activity	friends_groups	publish_checkins
	user_groups	friends_hometown	publish_stream
	user_hometown	friends_interests	read_friendlists
	user_interests	friends_likes	read_insights
	user_likes	friends_location	read_mailbox
	user_location	friends_notes	read_page_mailboxes
	user_notes	friends_online.presence	read_requests
	user_online.presence	friends_photo.video.tags	read_stream
	user_photo.video.tags	friends_photos	rsvp.event
	user_photos	friends_questions	share_item
	user_questions	friends_relationship.details	sms
	user_relationship.details	friends_relationships	status.update
	user_relationships	friends_religion.politics	video.upload
	user_religion.politics	friends_status	xmpp.login
	user_status	friends_subscriptions	
	user_videos	friends_website	
	user_website	friends_work.history	
	user_work.history		

124. As shown above, Graph API v.1.0's "Extended Profile Properties" encompassed certain categories of information about the downloading app user and that user's friends. Graph API v.1.0 allowed app developers to obtain those categories of information, which included: about me; activities; birthdays; check ins; education history; events; groups; hometown; interests; likes; location; notice; photos; questions; relationships; relationship details; religion

and politics; status; subscriptions; videos; websites; and work history.

125. On Graph API v.1.0, app developers could also ask Facebook's permission to access further categories of information called "Extended Permissions" which would allow even more access to users' and users' friends' information. Video information was also available to developers through at least seven different categories of data. These categories included: "users\_videos", "friends\_video"; "users\_subscriptions"; "friends\_subscriptions"; "users\_likes"; "friends\_likes"; and "read\_stream." Facebook set users' default app settings to allow sharing of six out of the seven of these categories.

126. According to Facebook's definition, the data queries "users\_videos" and "friends\_video" permissions allowed app developers to obtain "the videos the user has uploaded, and videos the user has been tagged in." Facebook set users' default "app settings" to allow all of this information to be shared with developers through a user's friend. Thus, any app developer who requested these permissions could have received video information from all users who had not changed the default settings.

127. The "users\_likes" and "friends\_likes" data categories allowed access "to the list of all of the pages the user [had] liked." Facebook defines "Facebook Pages" as "a public profile that allows anyone including artists, public figures, businesses, brands, organizations, and charities to create a presence on Facebook and engage with the Facebook community."

128. According to Facebook's S-1 filing in April 2012, "Examples of popular Pages on Facebook include Lady Gaga, Disney, and Manchester United, each of which has more than 20 million Likes." By March 31, 2012, "there were more than 42 million Pages with ten or more likes." Accordingly, users' likes would have included the Facebook pages for any movies, television shows, actors, production studios, etc. that the user had liked. Facebook set users' default "app settings" to allow this information to be shared to developers through a users' friend.

129. Finally, Facebook allowed app developers access to video information through the "read\_stream" query. Facebook's developer webpage defined this category as providing

“access to all the posts in the user’s News Feed and enables your application to perform searches against the user’s News Feed.” This information would include any videos uploaded by the user as well as any videos or video hyperlinks shared with a user. It would also include any and all posts by that user and shared with that user about videos. For instance, an app developer using this permission setting could see a user’s posted critique of a specific movie.

## **2. Cambridge Analytica Used Facebook’s API to Take Users’ Content and Information Without Their Knowledge Or Consent**

130. In 2007, when psychologists Michal Kosinski and David Stillwell from Cambridge University’s Psychometrics Centre began using a Facebook quiz they developed called “myPersonality” to study personality traits of consenting users. The app determined gender, age and sex, opening doors for psychologists to consider different ways to connect “likes” with personality traits. Their research received notice from the U.S. Defense Advanced Research Projects Agency (or “DARPA”). Kosinski and Stillwell published their findings in the Proceedings of the National Academy of Sciences in 2013.<sup>13</sup>

131. Researchers from Cambridge University used the myPersonality quiz to create a database “with profile information for over 6 million Facebook users. It has those users’ psychological profiles, their likes, their music listening, their religious and political views, and their locations, among other information. It says it can predict users’ leadership potential, personality, and ‘satisfaction with life.’”<sup>14</sup>

132. In 2013, Cambridge Analytica approached the myPersonality app team to get access to the app’s data but was turned down because of its political ambitions.<sup>15</sup> That same year,

---

<sup>13</sup> Eric Killelea, *Cambridge Analytica: What We Know About the Facebook Data Scandal*, Rolling Stone (Mar. 20, 2018) <https://www.rollingstone.com/culture/culture-news/cambridge-analytica-what-we-know-about-the-facebook-data-scandal-202308/>.

<sup>14</sup> Kashmir Hill, *The Other Cambridge Personality Test Has Its Own Database with Millions of Facebook Profiles*, Gizmodo (Mar. 22, 2018), <https://gizmodo.com/the-other-cambridge-personality-test-has-its-own-databa-1823997062>.

<sup>15</sup> Only after the Cambridge Analytica Scandal did Facebook reveal that data from myPersonality had been publicly available for years. Phee Waterfield & Timothy Revell, *Huge New Facebook Data Leak Exposed Intimate Details of 3M Users*, New Scientist (May 15, 2018),

Aleksandr Kogan and his company Global Science Research (“GSR”) created an application called “MyDigitalLife” (also known as “thisisyourdigitallife”). Facebook had begun collaborating with Kogan concerning Facebook data in 2012. The agreement that Kogan struck with Facebook in 2013 allowed Kogan to launch the MyDigitalLife app on the Facebook platform.<sup>16</sup>

133. Facebook’s ties with GSR run deep. One of GSR’s two co-founders, Joseph Chancellor, is an employee at Facebook, but was placed on administrative leave after the Cambridge Analytica Scandal was publicized in 2018.

134. MyDigitalLife marketed itself to Facebook users as a tool that would help them have a better understanding of their own personalities, and that would supply data for use by academic psychologists. The app prompted users to answer questions for a psychological profile. Questions focused on the so-called “Big Five” personality traits: extraversion, agreeableness, openness, conscientiousness, and neuroticism.

135. Through MyDigitalLife, Kogan gained access to the personal data of the approximately 300,000 Facebook users that downloaded the app. In Spring 2014, Kogan was approached by a SCL-affiliated contractor and was asked to provide consulting services. Kogan set up GSR to carry out the work. The project was intended to deliver to SCL personality scores matched to the voter registration file for several million people. Kogan authorized GSR’s Facebook app to collect data from app users about not just the user, but also the user’s friends. This data was then used to predict personality and then provided back to SCL.

136. In its “End User Terms and Conditions,” GSR informed users that UK law governed the rights concerning the MyDigitalLife app: “Your Statutory Rights: Depending on the server location, **your data may be stored** within the United States **or in the United**

---

<https://www.newscientist.com/article/2168713-huge-new-facebook-data-leak-exposed-intimate-details-of-3m-users/>.

<sup>16</sup> On August 22, 2018, Facebook notified 4 million users that their data was misused when myPersonality refused Facebook’s request for an audit. Ime Archibong, *An Update on Our App Investigation*, Facebook (Aug. 22, 2018), <https://newsroom.fb.com/news/2018/08/update-on-app-investigation/>.

**Kingdom.** If your data is stored in the United States, American laws will regulate your rights. If your data is stored within the United Kingdom (UK), British and European Union laws will regulate how the data is processed, even if you live in the United States. Specifically, data protection and processing falls under a law called the Data Protection Act 1998. Under British and European Union law, you are considered to be a ‘Data Subject’, which means you have certain legal rights. These rights include the ability to see what data is stored about you.”

137. Upon information and belief, at least part of the personal content stored by GSR was located in the UK and administered by Facebook Ireland, Inc. GSR represented to Facebook users that it was a “research organization” with a “registered office based at Magdalene College, Cambridge.” Publicized emails between Kogan and researchers at Cambridge demonstrate that Kogan used Cambridge’s UK-based servers for GSR. GSR made no secret of the blatantly commercial nature of its use of Facebook data. It states in its “End User Terms and Conditions” that it intended to “sell” and “license (by whatever means and on whatever terms)” the personal content it obtained through the MyDigitalLife app. Facebook was provided with GSR’s terms of service and thus was given constructive if not actual notice that GSR was selling user content and information. Kogan has stated that he “never heard a word” from Facebook concerning his intent to “sell” data even though he had publicly posted his intention for a year and a half.

138. Kogan and GSR actively began their relationship with Cambridge Analytica in 2014 and 2015. During this time, Kogan and GSR provided Cambridge Analytica with much more than the personal content and information of the Facebook users who had downloaded the MyDigitalLife app. Graph API v.1.0, which Facebook was still using, allowed the app to access the data that users’ *friends* had shared with them. Through this platform, Facebook gave Kogan and GSR, and thus Cambridge Analytica and other third parties like the University of Toronto and the University of British Columbia, the content and information of more than 50 million additional people who, according to Facebook, “had their privacy settings set to allow it.”

139. Facebook now estimates that up to 87 million Facebook users affected by this scheme, only approximately 300,000 of them had downloaded the MyDigitalLife app—and



those users had agreed to share only their own content and information for the limited purposes associated with the app. The Company admits, however, that historical logs of users' privacy settings are scant. Upon information and belief, at least the photos shared with Cambridge Analytica were stripped of identifying information that would have communicated the privacy restrictions of users' friends. About 1,500 people also gave the app access to their private messages, and people who sent or received messages with those people potentially had their private messages accessed as well.

140. In addition to supplying Cambridge Analytica with fresh Facebook user data on an ongoing basis, Kogan and GSR, at Cambridge Analytica's request, also performed modelling work on the data. Communications disclosed by Cambridge Analytica personnel demonstrate Kogan's active role in this modeling.

141. CEO Zuckerberg has admitted that Facebook became aware that Kogan and GSR had misused data in 2015 and conducted an investigation.<sup>17</sup> Defendant Facebook states that it contacted Kogan following the publication of the *Guardian* article in 2015.

142. At minimum, Facebook became aware that GSR sold Facebook data containing personal content by March 2016, when, while negotiating a settlement of claims with Kogan, Facebook was informed that Kogan had made roughly \$800,000 re-selling Facebook user data. Facebook failed to determine at that time the scope and extent of the content and information GSR had obtained. Indeed, Facebook waited over two years to make any type of public disclosure.

143. Kogan initially used the Facebook data that he had obtained in 2012 and subsequently to co-author a number of papers that had obvious commercial purposes and applications. Kogan co-authored papers entitled "Tracing Cultural Similarities and Differences in Emotional Expression through Digital Records of Emotions," "Happiness Predicts Larger Online Social Networks for Nations and Individuals Low, but not High, in Consumeristic Attitudes and

---

<sup>17</sup> *Facebook's Use and Protection of User Data: Hearing Before the H. Energy and Commerce Comm.*, 2018 WL 1757479, at 22-23 (Apr. 11, 2018) (statement of Mark Zuckerberg).

Behaviors,” “Silk Road to Friendships: Economic Cooperation is Associated with International Friendships around the World,” “Big Data Public Health: Online Friendships can Identify Populations At-Risk of Physical Health Problems and All-Causes Morbidity,” and “Donations Predict Social Capital Gains for Low SES, But Not High SES Individuals and Countries.”<sup>18</sup>

144. Christopher Wylie, a former Cambridge Analytica contractor, has recently revealed how the data mining process at Cambridge Analytica worked: By getting access to Facebook users’ “profiles, likes, even private messages, [Cambridge Analytica] could build a personality profile on each person and know how best to target them with messages.”<sup>19</sup> Facebook users’ profiles “contained enough information, including places of residence, that [Cambridge Analytica] could match users to other records and build psychographic profiles.”<sup>20</sup> Mr. Wylie has said: “We exploited Facebook to harvest millions of people’s profiles. And built models to exploit what we knew about them and target their inner demons. That was the basis the entire company was built on.”<sup>21</sup>

145. The figure below was created by the United Kingdom Information Commissioner’s Office (“ICO”), which is a government agency set up to uphold information rights in the public interest, and to promote openness by public bodies and data privacy for individuals. The figure describes how Cambridge Analytica accessed and harvested the content

---

<sup>18</sup> Def. Facebook, Inc.’s Resps. & Objs. to Pls.’ First Set of Interrogs. at pp. 7-8 (Sept. 7, 2018).

<sup>19</sup> Parmy Olson, *Face-To-Face With Cambridge Analytica’s Elusive Alexander Nix*, Forbes (Mar. 20, 2018), <https://www.forbes.com/sites/parmyolson/2018/03/20/face-to-face-with-cambridge-analytica-alexander-nix-facebook-trump/#54972c48535f>.

<sup>20</sup> Matthew Rosenberg et al., *How Trump Consultants Exploited the Facebook Data of Millions*, N.Y. Times (Mar. 17, 2018), <https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html>.

<sup>21</sup> Carole Cadwalladr & Emma Graham-Harrison, *Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach*, Guardian (Mar. 17, 2018), <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>.





146. As outlined above, the ICO has found that GSR obtained the following information from users who downloaded the MyDigitalLife app: “Public Facebook profile, including their name and gender; Birth date; Current city, if the user had chosen to add this information to their profile; Photographs in which the users were tagged; Pages that the users had liked Posts on the users’ timelines; News feed posts; Friends lists; Email addresses; and Facebook messages.”<sup>23</sup>

147. The ICO reports that GSR obtained the following information from the downloading users’ friends: “Public Facebook profile, including their name and gender; Birth date; Current city if the friends had chosen to add this information to their profile; Photographs in which the friends were tagged; and Pages that the friends had liked.”<sup>24</sup>

148. GSR obtained access to users’ and users’ friends likes.<sup>25</sup> This information would include specific video information about these users. GSR shared this like information with Cambridge Analytica.<sup>26</sup> Thus, Facebook allowed GSR to access and share the specific video preferences of its users through this “likes” information.

149. GSR obtained access to the “posts on the users timeline” for users who installed the MyDigitalLife app.<sup>27</sup> This access would have been available under the “read\_stream” query. Facebook claims that they denied Aleksandr Kogan’s request to access this query.<sup>28</sup> But this

---

<sup>22</sup> Information Commissioner’s Office, *Investigation Into the Use of Data Analytics in Political Campaigns – Investigation Update*, (July 11, 2018), (“ICO Report”) at 17, <https://ico.org.uk/media/action-weve-taken/2259371/investigation-into-data-analytics-for-political-purposes-update.pdf>.

<sup>23</sup> ICO Report 19-20.

<sup>24</sup> *Id.*

<sup>25</sup> *Id.*

<sup>26</sup> *Id.*; see also Digital, Culture, Media and Sport Committee (House of Commons), Examination of Witness Dr. Aleksandr Kogan at Q1930, Apr. 24, 2018, <http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/digital-culture-media-and-sport-committee/fake-news/oral/81931.html>.

<sup>27</sup> ICO Report 19-20.

<sup>28</sup> Def. Facebook, Inc.’s Resps. & Objs. to Pls.’ First Set of Interrogs. at pp. 6-7 (“Dr. Kogan’s App Review application sought extended permissions for the App . . . Facebook rejected Dr.

claim contradicts the UK’s ICO’s published report on this matter. Through this query, GSR obtained additional access to any information about a user’s video preferences posted on that user’s timeline.

150. After the Cambridge Analytica Scandal became public in March 2018, Facebook announced that it was suspending Cambridge Analytica and its parent company, Strategic Communication Laboratories (“SCL”), from Facebook. It stated that, in 2015, it learned it had been lied to by Dr. Kogan and that Kogan had violated Facebook’s Platform Policies—contracts between Facebook and third-party apps—“by passing data from an app that was using Facebook Login to SCL/Cambridge Analytica.”<sup>29</sup> Seeking to avoid liability, SCL and its related entities, like Cambridge Analytica, have all filed for bankruptcy, as has GSR.

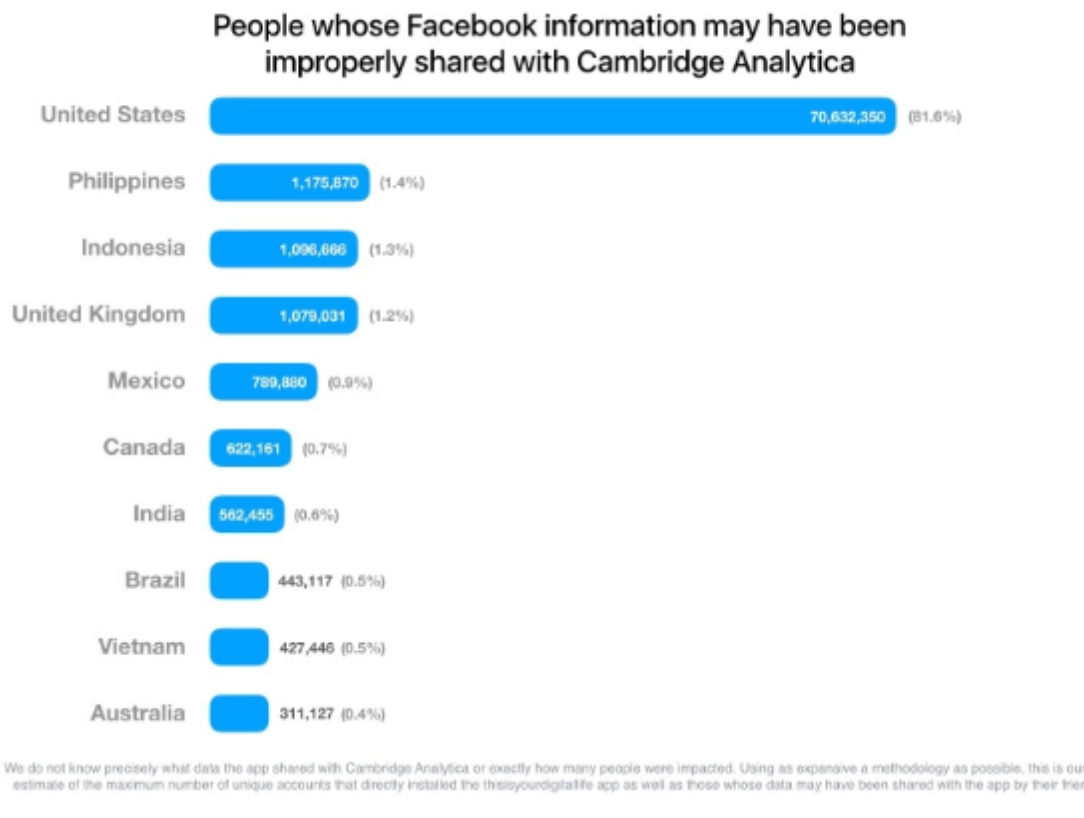
151. On April 4, 2018, Facebook released the following statement: “In total, we believe the Facebook information of up to 87 million people—mostly in the United States—may have been improperly shared with Cambridge Analytica.” Facebook also released a country-by-

---

Kogan’s application the next day, stating that the App would not be using the data requested to enhance the user’s in-app experience.”).

<sup>29</sup> Paul Grewal, *Suspending Cambridge Analytica and SCL Group From Facebook*, Facebook (Mar. 16, 2018), <https://newsroom.fb.com/news/2018/03/suspending-cambridge-analytica/>.

country breakdown of the millions of users affected by the GSR app, pictured below:



152. On May 1, 2018, Facebook updated this blog post to include a state-by-state breakdown of the millions of users who may have had their information shared with Cambridge

Analytica, shown below:

**State-by-State Breakdown of People Whose Facebook Information May Have  
Been Improperly Shared with Cambridge Analytica**

State	Total Impacted Users	State	Total Impacted Users
California	6,787,507	Oklahoma	962,267
Texas	5,655,677	Mississippi	871,695
Florida	4,382,697	Arkansas	829,598
New York	4,368,051	Oregon	798,959
Pennsylvania	2,960,311	Iowa	685,777
Illinois	2,949,469	Connecticut	655,062
Ohio	2,927,388	Kansas	647,563
Georgia	2,857,971	Nevada	631,062
North Carolina	2,521,064	Utah	619,277
Michigan	2,414,438	West Virginia	557,046
Tennessee	1,783,650	Nebraska	384,815
Virginia	1,709,835	New Mexico	348,472
Indiana	1,698,230	District of Columbia	345,652
New Jersey	1,605,868	Idaho	326,248
Missouri	1,574,855	Maine	309,546
Washington	1,434,126	Hawaii	279,583
Alabama	1,385,169	New Hampshire	258,772
Kentucky	1,310,682	Rhode Island	239,240
Massachusetts	1,265,149	Delaware	201,553
Louisiana	1,263,851	Montana	183,744
South Carolina	1,258,400	South Dakota	153,382
Arizona	1,252,103	North Dakota	143,243
Wisconsin	1,200,116	Alaska	139,997
Maryland	1,102,857	Vermont	135,960
Minnesota	1,032,670	Wyoming	112,440
Colorado	966,492		

153. In his April 2018 testimony to the U.K. House of Commons, Facebook Chief Technology Officer Mike Schroepfer testified that Facebook did not read terms and conditions of

any developer's apps that were put on Facebook. In this litigation, in its interrogatory responses, Facebook has averred that it could not possibly have read the terms and conditions of these apps, because there were millions of them.<sup>30</sup> This is one more indication that Facebook did not protect user content and information once it gave access to app developers.

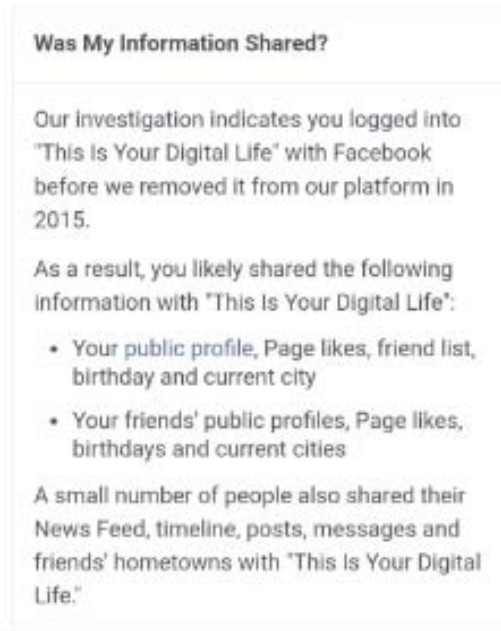
154. On April 9, 2018, with a notification at the top of News Feeds, Facebook began notifying individual users if their data had been shared with Cambridge Analytica. For example, Plaintiff Fischer received a notification from Facebook in April 2018 that she had logged into "This is Your Digital Life" and her public profile, page likes, friend list, birthday, current city, friend's public profiles, friends' page likes, friends' birthdays, and friends' current cities were likely shared with "This is Your Digital Life." The notification also explained that a small number of people also shared their News feed, timeline, posts, messages, and friends' hometowns with "This is Your Digital Life."

155. Plaintiff Jarvimaki, as another example, received a notification from Facebook in April 2018 that one of her Facebook friends had logged into "This is Your Digital Life" and therefore, her public profile, page likes, friend list, birthday, and current city were likely shared with "This is Your Digital Life." The notification also explained that a small number of people also shared their News Feed, timeline, posts, friends' hometowns, and messages with "This is Your Digital Life," which may have included posts and messages from Plaintiff Jarvimaki as well as her hometown.

156. The notification that Plaintiffs Fischer and Jarvimaki received looked like this:

---

<sup>30</sup> Def. Facebook, Inc.'s Resps. & Objs. to Pls.' First Set of Interrogs. at p. 20.



157. On April 22, 2018, Dr. Kogan finally broke his silence in an interview with CBS News Correspondent Lesley Stahl on 60 Minutes. Kogan stated he had terms of service up on his application for a year and a half—terms providing that he could sell the data he obtained through the app—and yet Facebook never enforced its agreement with Kogan or its rules against selling data during this time. Kogan also explained that the ability to gather people’s Facebook friends’ data without their permission was a Facebook core feature, available to anyone who was a developer. He explained that there are likely tens of thousands of applications that did what he did, as this was not a bug, but a feature of which Facebook was aware.

158. Among scores of other regulators, the Justice Department and FBI are now investigating Cambridge Analytica, which filed for Chapter 7 bankruptcy on May 17, 2018.

159. Further, in the wake of the Cambridge Analytica Scandal, Facebook suspended two other companies from its platform in April 2018 for improper data collection: Canadian consulting firm AggregateIQ and CubeYou.

160. Facebook suspended AggregateIQ based on reports that it is affiliated with SCL. Further, Wylie told *The Observer* in March that AggregateIQ was originally established to assist



with SCL's projects. It has been reported that AggregateIQ was instrumental in analyzing voter data for the Brexit campaigns.

161. Facebook's suspension of CubeYou was based on evidence provided by CNBC, which showed that CubeYou had misled users by collecting data from quizzes inaccurately labeled "non-profit academic research" and then selling the findings to marketers.

### **3. The Cambridge Analytica Scandal Has Triggered Seriatim Revelations by Facebook of Third Party Abuse of User Content and Information**

162. As Facebook admitted in its April 26, 2018 SEC Quarterly Report, GSR and Cambridge Analytica are not the only entities that have used Facebook's API to obtain unauthorized access to, and make unauthorized use of, Facebook users' content and information. As Facebook noted in the Quarterly Report, "We anticipate that we will discover and announce additional incidents of misuse of user data or other undesirable activity by third parties. We may also be notified of such incidents or activity via the media or other third parties. Such incidents and activities may include the use of user data in a manner inconsistent with our terms or policies, the existence of false or undesirable user accounts, election interference, improper ad purchases, activities that threaten people's safety on- or offline, or instances of spamming, scraping, or spreading misinformation."

163. Since the public learned of the Cambridge Analytica Scandal, Facebook has since said it has investigated thousands of apps and has suspended 400 of them as a result of this investigation. Facebook states that it suspended these apps "due to concerns around the developers who built them or how the information people chose to share with the app may have been used."

164. Facebook has also revealed that some companies were granted special access to Graph API v1.0 beyond May 2015. In response to questions posed by the U.S. House of Representative on June 29, 2018, Facebook stated that a set of companies were "given a one-



time extension of less than six months beyond May 2015 to come into compliance” with Facebook’s new API for apps.<sup>31</sup>

165. The list of companies includes:
- ABCSocial, ABC Television Network
  - Actiance
  - Adium
  - Anschutz Entertainment Group
  - AOL
  - Arktan / Janrain
  - Audi
  - biNu
  - Cerulean Studios
  - Coffee Meets Bagel
  - DataSift
  - Dingtone
  - Double Down Interactive
  - Endomondo
  - Flowics, Zauber Labs
  - Garena
  - Global Relay Communications
  - Hearsay Systems
  - Hinge
  - HiQ International AB
  - Hootsuite
  - Krush Technologies
  - LiveFyre / Adobe Systems
  - Mail.ru
  - MiggoChat
  - Monterosa Productions Limited
  - never.no AS
  - NIKE
  - Nimbuzz
  - Nissan Motor Co. / Airbiquity Inc.
  - Oracle
  - Panasonic
  - Playtika
  - Postano, TigerLogic Corporation
  - Raidcall
  - RealNetworks, Inc.

---

<sup>31</sup> Letter from Facebook, Inc. to Chairman Greg Walden, Ranking Member Frank Pallone, Energy & Commerce Committee, and U.S. House of Representatives, *Facebook’s Response to House Energy and Commerce Questions for the Record* (June 29, 2018) at Pallone, Jr. § 4 ¶ 6.

- RegED / Stoneriver RegED
- Reliance/Saavn
- Rovi
- Salesforce/Radian6
- SeaChange International
- Serotek Corp.
- Shape Services
- Smarsh
- Snap
- Social SafeGuard
- Socialeyes LLC
- SocialNewsdesk
- Socialware / Proofpoint
- SoundayMusic
- Spotify
- Spredfast
- Sprinklr / Sprinklr Japan
- Storyful Limited / News Corp
- Tagboard
- Telescope
- Tradable Bits, TradableBits Media Inc.
- UPS
- Vidpresso
- Vizrt Group AS
- Wayin

166. During this six-month extension these companies continued to have access to the content and information of users and users’ friends. Facebook has not clarified why this group of companies were given special access to users’ content and information.

167. Facebook has also listed five companies that “could have accessed limited friends’ data as a result of API access they received in the context of a beta test.”<sup>32</sup> These companies include:

- Activision / Bizarre Creations
- Fun2Shoot
- Golden Union Co.
- IQ Zone / PicDial
- PeekSocial

---

<sup>32</sup> Letter from Facebook, Inc. to Chairman Greg Walden, Ranking Member Frank Pallone, Energy & Commerce Committee, and U.S. House of Representatives, *Facebook’s Response to House Energy and Commerce Questions for the Record* (June 29, 2018) at Pallone, Jr. § 4 ¶ 7.

168. Facebook has not provided an explanation for why these five companies received this special access.

**4. Facebook Also Enabled Device Makers and Other Business Partners to Access Users' Content And Information Through Friends**

169. Facebook started forming partnerships with electronic device makers, or “device-integrated APIs,”<sup>33</sup> in 2007. Following the Congressional inquiry into the Cambridge Analytica Scandal, Facebook identified 52 data-sharing partnerships with companies such as Apple, Amazon, Blackberry, Microsoft and Samsung which also allowed user content and information to be shared. Critically, those agreements permitted data sharing that was not subject to users' privacy settings. Moreover, Facebook never told users that it was sharing data with these third parties.<sup>34</sup>

170. Device makers, like app developers, use APIs engineered by and in the control of Facebook to collect Facebook user data. Facebook's “device-integrated APIs that allowed companies to recreate Facebook-like experiences for their individual devices or operating systems. Over the last decade, around 52 companies have used them—including many household names such as Amazon, Apple, Blackberry, HTC, Microsoft and Samsung.”<sup>35</sup> Facebook's goal was to make Facebook available not only on desktop computers, but also on users' mobile phones, smart TVs, game consoles, and other devices. Even before users could download the Facebook application on their phones, Facebook partnered with device manufacturers to incorporate parts of the social network into the devices themselves. For example, Facebook allowed manufacturers to integrate “like” buttons, photo sharing, and friend lists into their

---

<sup>33</sup> Ime Archibong, *Why We Disagree with The New York Times*, Facebook (June 3, 2018), <https://newsroom.fb.com/news/2018/06/why-we-disagree-with-the-nyt/>.

<sup>34</sup> Gabriel J.X. Dance et al., *Facebook Gave Device Makers Deep Access to Data on Users and Friends*, N.Y. Times (June 3, 2018), <https://www.nytimes.com/interactive/2018/06/03/technology/facebook-device-partners-users-friends-data.html>.

<sup>35</sup> Ime Archibong, *Why We Disagree with The New York Times*, Facebook (June 3, 2018), <https://newsroom.fb.com/news/2018/06/why-we-disagree-with-the-nyt/>.

devices.<sup>36</sup>

171. In 2008, Microsoft entered into a partnership with Facebook that allowed Microsoft-powered devices to add contacts and friends and receive notifications, among other capabilities.<sup>37</sup> Apple relied on private access to Facebook data for features that enabled users to post photos to the social network without opening the Facebook application.<sup>38</sup> Blackberry used Facebook data to give its own customers access to their Facebook network and messages. But Blackberry has recently stated that it “did not collect or mine the Facebook data of [its] customers.”<sup>39</sup> As with the user content and information shared with app developers, these third parties gained access to users’ content and information not through a direct relationship between a user and the third party, but through a user’s friends.

172. Sandy Parakilas, a whistleblower and a former operations manager at Facebook, asserts that the same “feature” is behind both the Cambridge Analytica Scandal and Facebook’s data sharing with device makers. In both cases, “developers had access” to a user’s friend data—and “[a]llowing access to data from friends of the user is the same feature that let Aleksandr Kogan get access to 87M profiles with only 270k people using his app, which he then passed on to Cambridge Analytica.”<sup>40</sup> Indeed, Parakilas equated device makers to “apps.”

173. The *New York Times* has reported that “[s]ome device partners can retrieve Facebook users’ relationship status, religion, political leaning and upcoming events, among other

---

<sup>36</sup> Gabriel J.X. Dance et al., *Facebook’s Device Partnerships Explained*, N.Y. Times (June 4, 2018), <https://www.nytimes.com/2018/06/04/technology/facebook-device-partnerships.html>.

<sup>37</sup> Gabriel J.X. Dance et al., *Facebook Gave Device Makers Deep Access to Data on Users and Friends*, N.Y. Times (June 3, 2018), <https://www.nytimes.com/interactive/2018/06/03/technology/facebook-device-partners-users-friends-data.html>.

<sup>38</sup> *Id.*

<sup>39</sup> *Id.*

<sup>40</sup> Sandy Parakilas (@mixblendr), Twitter (June 4, 2018, 12:44 AM), <https://twitter.com/mixblendr/status/1003542895507501057>, <https://twitter.com/mixblendr/status/1003542896732237824>.

data.”<sup>41</sup> Further, “[t]ests by The Times showed that the partners requested and received data in the same way other third parties did.”<sup>42</sup>

174. As set forth below, users could not have expected to know that these third parties had access to their content and information in abrogation of their privacy settings.

**5. Facebook Disregarded Friends’ Privacy Settings When Transferring Data to Third Parties Through Graph API v. 1.0**

175. Upon information and belief, friends’ photos did not retain their privacy restrictions when they passed into the possession of third parties who accessed content through Graph API v. 1.0. Those third parties, unaware of any privacy restrictions, might then share them with the broader public. Thus, photos sent to friends with even the most restrictive privacy settings, save making them available only to yourself, were shared beyond the scope of their consent.

176. The privacy restrictions are contained in electronic content, known as “metadata,” which is electronically associated with each photo as the photo is posted. Photo metadata also reveals when and where photos are taken. Curiously, when Facebook made photos available Graph API v. 1.0, the metadata reflecting user’s privacy designations associated with photos was not provided to third parties, even though other photo metadata was. Because the privacy restrictions metadata was blocked from the associated photos, third parties were unable to verify that a user’s privacy settings allowed for a given photo to be shared and, therefore, could not confirm that they were adhering to users’ privacy settings as required by Facebook’s Platform Policy.

177. Upon information and belief, Facebook alone was responsible for loading content into Graph API v. 1.0. The removal of users’ privacy metadata from photos, which persisted from at least 2012-2014, thwarted users’ affirmative privacy designations as to those photos by

---

<sup>41</sup> Gabriel J.X. Dance et al., *Facebook Gave Device Makers Deep Access to Data on Users and Friends*, N.Y. Times (June 3, 2018), <https://www.nytimes.com/interactive/2018/06/03/technology/facebook-device-partners-users-friends-data.html>.

<sup>42</sup> *Id.*

allowing third parties to access users' photos without providing users' corresponding privacy settings. Thus, Facebook failed to provide third parties with the crucial information that would have allowed app third parties to verify that they were accessing users' photos in compliance with users' privacy settings.

178. Certainly with regard to apps, Facebook's actions violated its agreement with users. Namely, "[w]e require applications to respect your privacy...."<sup>43</sup> Upon information and belief, Facebook was notified by at least one app developer, of the missing metadata as early as 2012.

179. Upon information and belief, Facebook deliberately allowed app developers to access users' photos, without regard to their privacy settings, in order to maximize the amount of content and information available. Indeed, if the metadata containing privacy restrictions had been made available through Graph API v. 1.0, it would have greatly diminished app developers' ability to use photos. The failure to provide this metadata served Facebook's plan for growth-at-all-costs. That is, here as elsewhere, Facebook's actual practice undermined the policy to which it paid lip service, egregiously harming users and greatly benefiting Facebook.

**C. Facebook Made It Unreasonably Confusing and Burdensome for Users to Prevent the Sharing of Their Content and Information with Third-party Applications.**

180. Facebook's unauthorized disclosure of users' content and information is bad enough. What makes it even worse were the barriers Facebook placed in the way of users who wanted to limit what third parties could access.

181. Facebook created "Privacy Settings" that it told users to employ to control the kinds of content and information they shared with others. Conveniently for users, these Privacy Settings were in a reasonably accessible location on Facebook.

182. The problem was that the Privacy Settings did not control the kinds of content and information that Facebook allowed *applications* to access. The content and information that

---

<sup>43</sup> *Statement of Rights and Responsibilities*, Facebook (June 8, 2012), <https://www.facebook.com/legal/terms> [<https://web.archive.org/web/20121205191915/https://www.facebook.com/legal/terms>].

applications could access was governed by a completely separate set of controls—controls that Plaintiffs will refer to here as “App Settings.” And while Facebook made Privacy Settings accessible, it buried App Settings within its website so effectively that all but the most sophisticated or intrepid users would not know they even existed.

183. Moreover, the App Settings were set by default to *share* all content with third-party applications, not to prevent sharing. By establishing that default setting, Facebook created consent instead of seeking it.

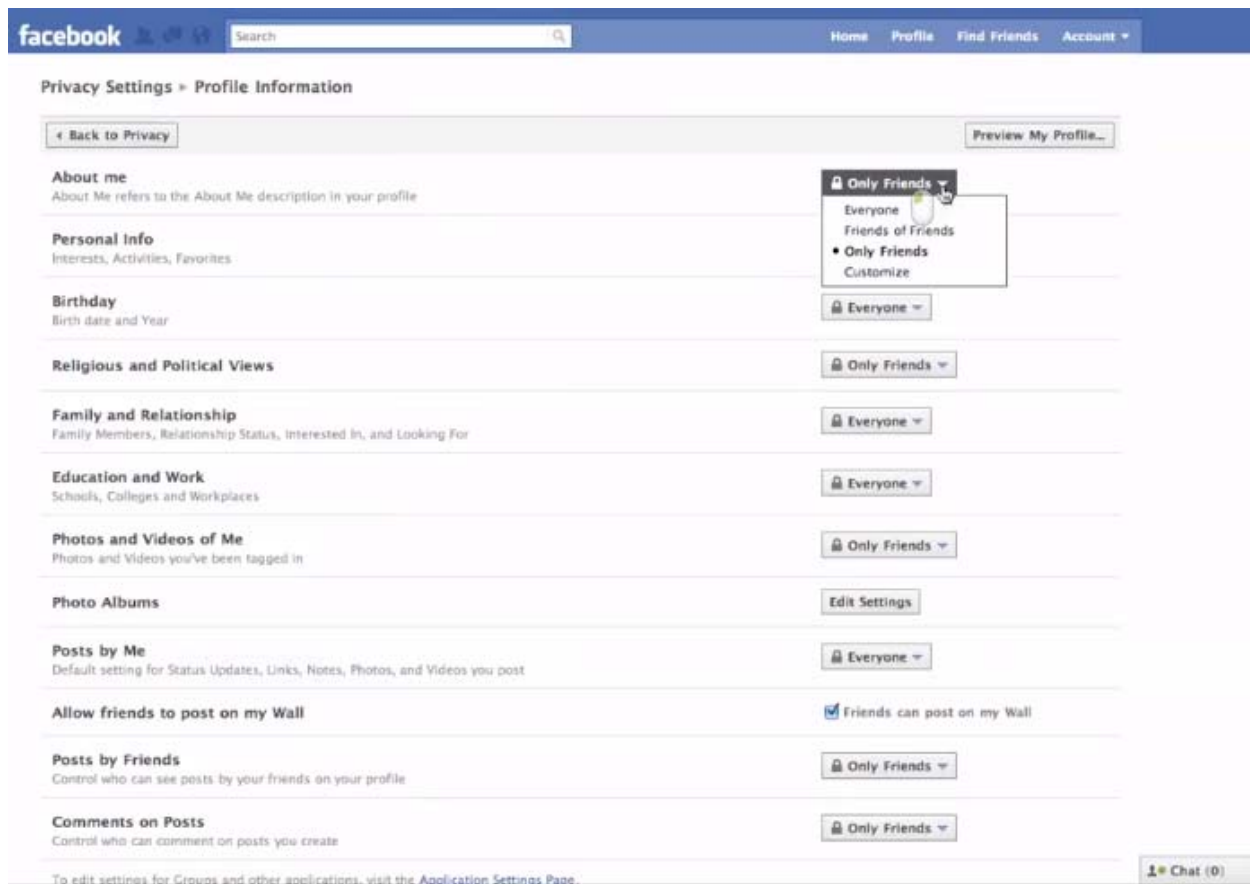
**1. Facebook’s “Privacy Settings” Misled Users About How to Control the Information and Content That They Shared with Applications.**

184. During the whole Class Period, Facebook’s “Privacy Settings” screen seemingly allowed a user to exert control over what information she shared with third parties.

185. For example, the screenshot of this “Privacy Settings” page from 2010 shown below offers a list of the categories of information. From this menu, the user can seemingly choose a specific audience to share this information with. Clicking the dropdown arrow next to each category allows users to specify whether the information is shared with “Everyone,” “Friends,” “Friends of Friends,” or to choose their own customized audience list.<sup>44</sup>

---

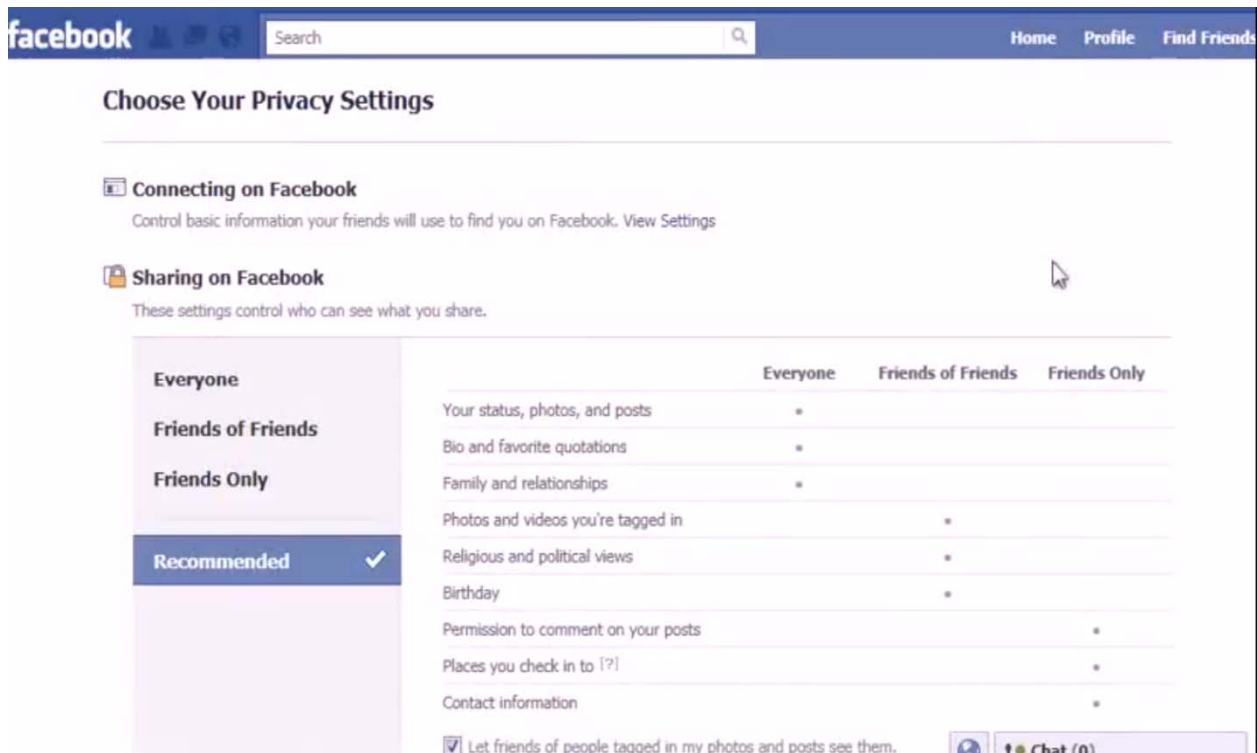
<sup>44</sup> Aarpwi, *FB Privacy Settings*, YouTube (Apr. 6, 2010), <https://www.youtube.com/watch?v=HRhB3R9DTNo>.



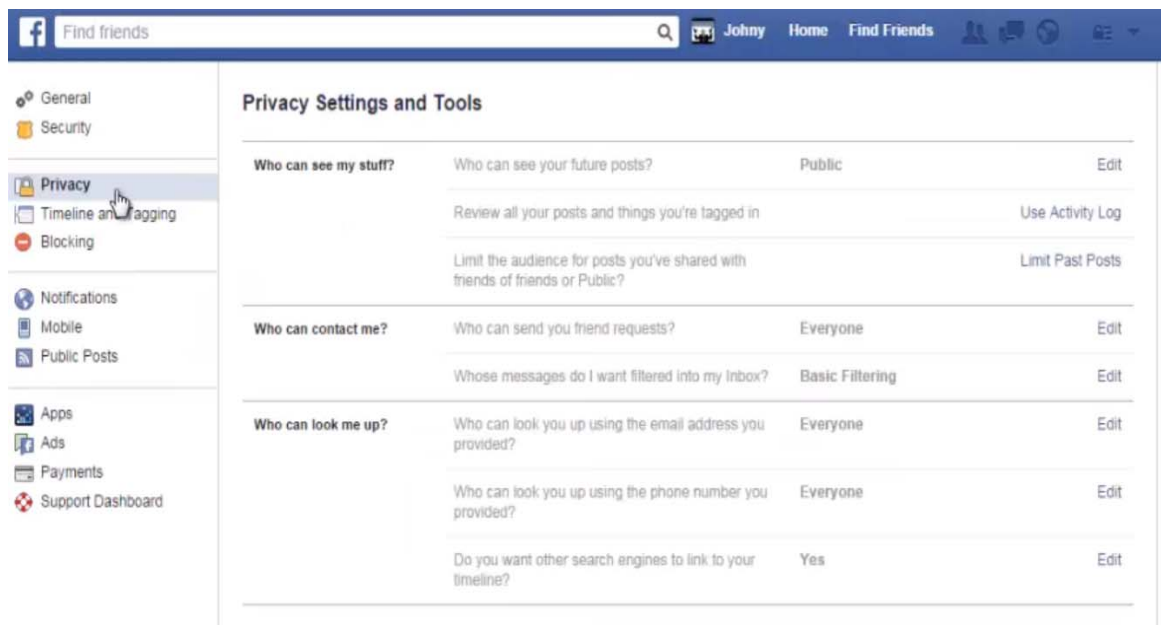
186. This screen changed slightly, to the display shown below, around 2010 to 2011.<sup>45</sup> Like the previous screen, this webpage seemingly allowed users to choose who can see their content and information.

<sup>45</sup> Kvchosting, *How to Manage Your Privacy Settings on Facebook*, YouTube (Mar. 25, 2013), <https://www.youtube.com/watch?v=O378rrYcjlC>.





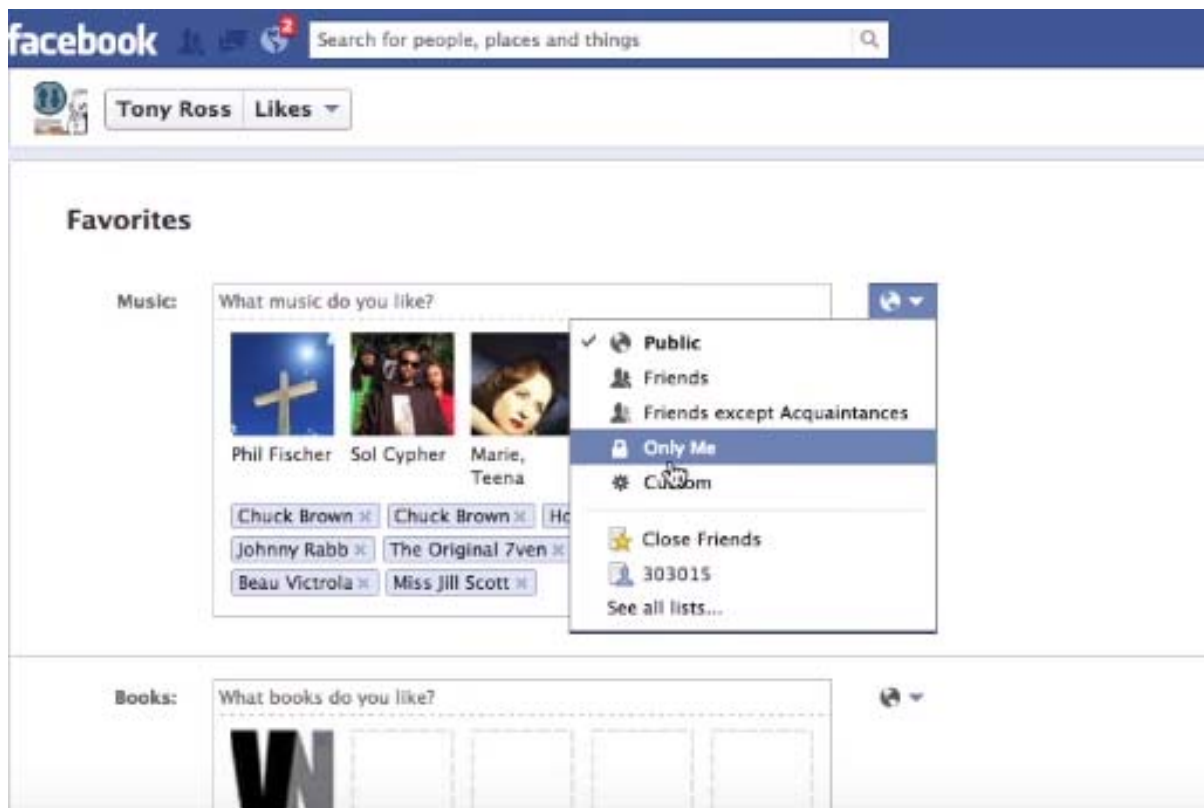
187. At some time in 2012 to 2013, the display changed again to the display shown below. This screen stayed substantially the same until April 2018.



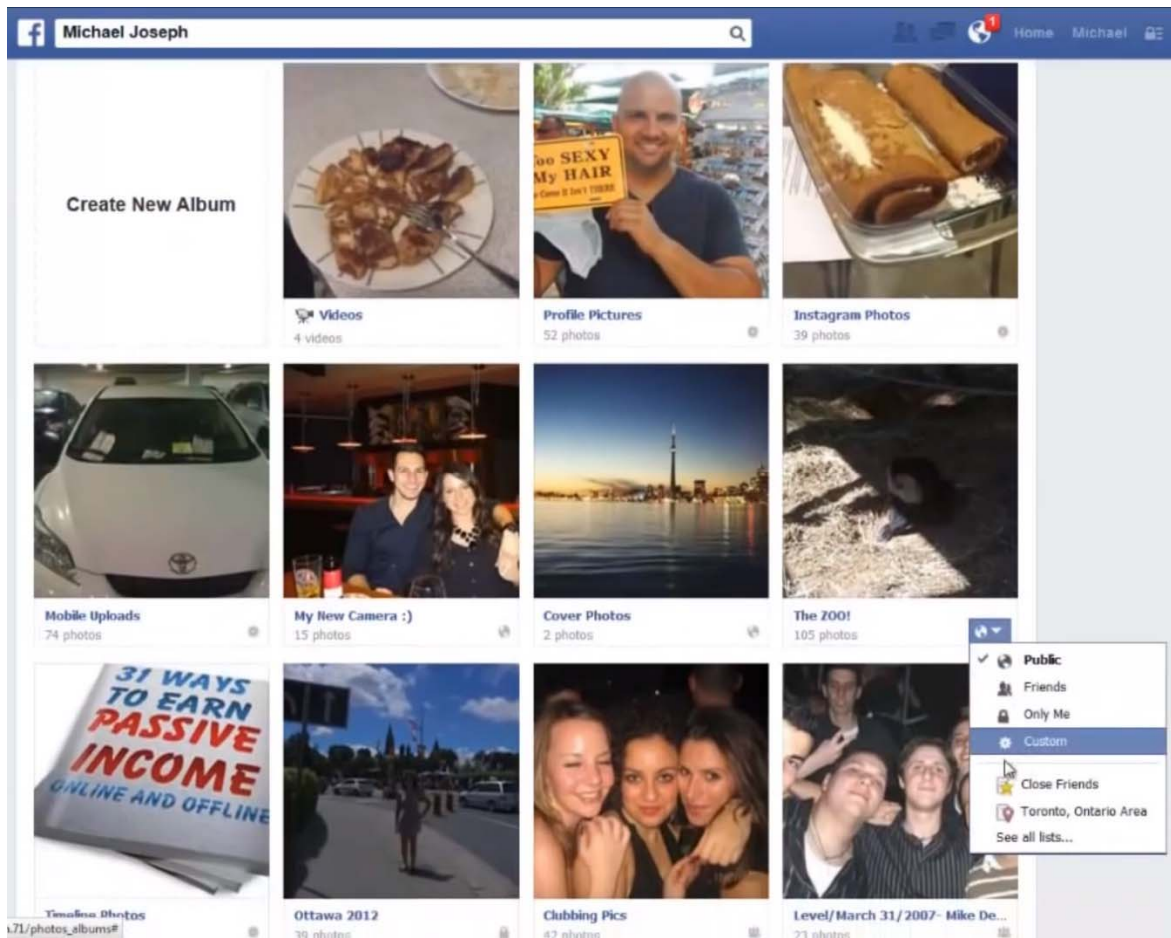
188. Like the displays above, during this period, users could select the edit button next to each category of information. This would then allow the user to choose the exact audience that could view the user's posts. For each "Privacy Setting" depicted above, users could click a

dropdown menu and restrict access to specified users, e.g., “Only Friends,” or “Friends of Friends.”

189. Users could also access this type of control for each individual category of information displayed on their Facebook profile (e.g., books, movies, etc.). For example, a user who wanted to hide her likes could locate the “likes” category on their public profile and select an audience dropdown menu next to each “likes” category. This menu gave users the following options for whom the information could be shared with: “Public,” “Friends,” “Only Me,” and “Custom.”



190. Facebook also seemingly offered users’ privacy controls over their photos. Users could set entire photo albums as well as individual photos to a specific audience. Examples are shown below:





191. Just like the privacy settings page, each of these individual categories purports to give a user control. In actuality, only the “only me” selection would have limited third-party applications from accessing the user’s information through her friends.

**2. To Control Sharing with Applications, Facebook Required Users to Hunt for, Find, and Change the Default Preferences of Their App Settings**

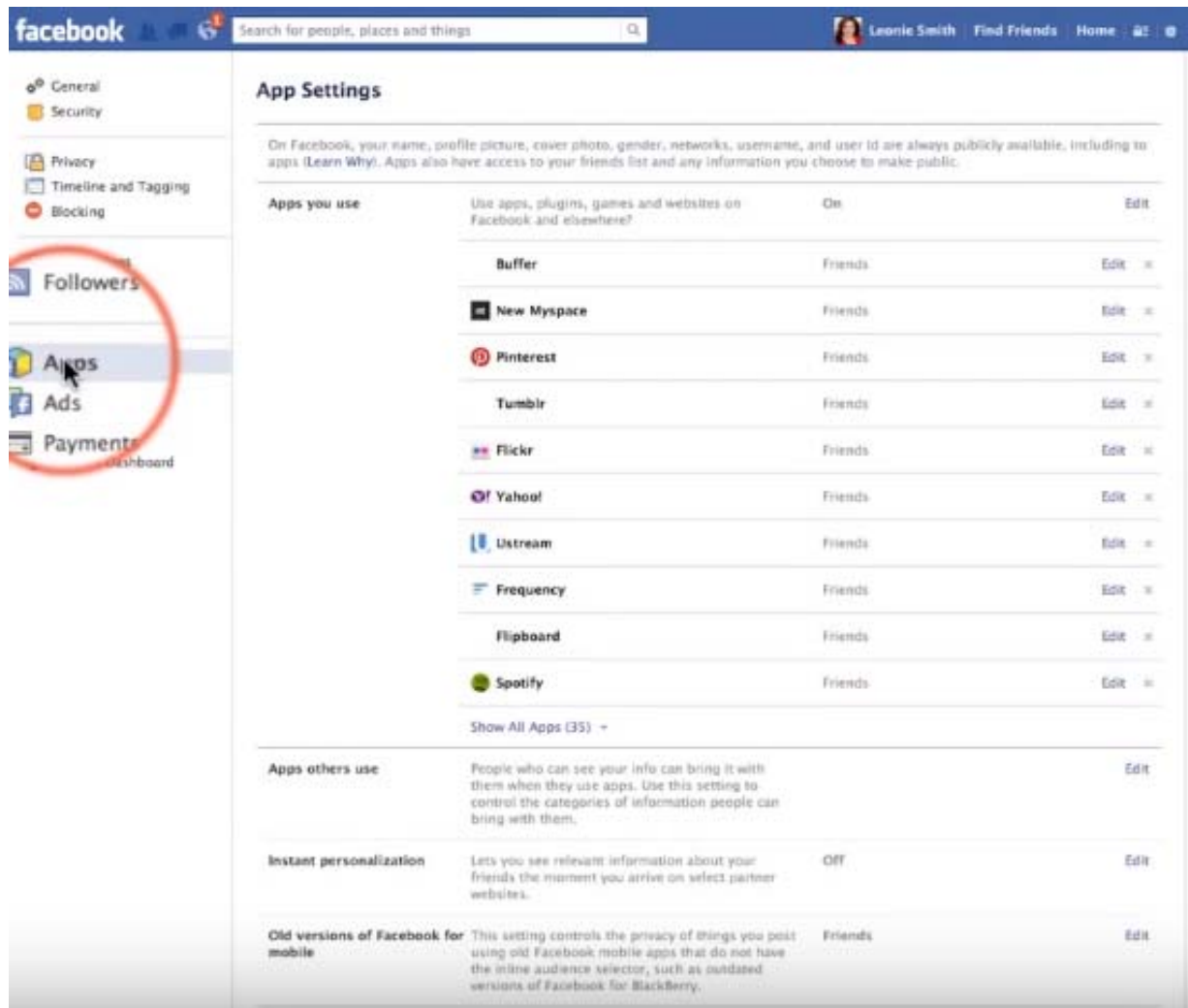
192. To prevent their information from being shared with applications through their friends, users needed to access their App Settings.

193. To access App Settings, this panel, a user would first need to access the Settings webpage. On that webpage, a user would need to click a hyperlink to “Apps” (during the Class Period, this link has also been labeled “Applications” and “Applications and Websites”).

194. After accessing the App Settings webpage, a user would then need to click the “Edit Settings” link next to the subheading “Apps others use.”<sup>46</sup> This subheading is described with these words: “People who can see your info can bring it with them when they use apps. Use

<sup>46</sup> See Leonie Smith, *Advanced Privacy Settings for Facebook 2013-2014*, YouTube (Jan. 17, 2013), <https://www.youtube.com/watch?v=OPRFQyGq-yM>.

this setting to control the categories of information people can bring with them.”<sup>47</sup>



195. A user would be able to alter their application-related privacy settings only after clicking the “edit” link.

196. The default “Apps others use” controls allowed the sharing of over fifteen categories of information. The default settings for every user allowed third parties access to the following categories of information: Bio; Birthday; Family and relationships; My website; If I’m online; My status updates; My photos; My videos; My links; My notes; Hometown; Current city; Education and work; Activities, interests, things I like; and My app activity. These default

<sup>47</sup> *Id.*

settings are shown below:



197. Each of these controls corresponds to a category of content and information that app developers could access using Graph API v.1.1.0.

198. To change her settings, a user would have to click each individual box and click “Save Changes.” In total, the user would have had to make twenty separate clicks to prevent Facebook from sharing these categories of content and information with third parties.

199. Even if a user un-checked each of these boxes, Facebook would still share that user’s friend list, gender, and other information that the user had made public. The only way to turn access off to third parties entirely was to turn off access to all applications. Yet, by default, applications were turned on. Thus, a user who had never accessed or signed up for an application still would have shared over fifteen categories of their information to third parties.

200. To turn off applications entirely, a user would need to go the App Settings page, go to the “Apps you use” subheading, and click the “edit” link next to that subheading. This would bring up the following disclosure:



## App Settings

On Facebook, your name, profile picture, cover photo, gender, networks, username, and user id are always publicly available, including to apps ([Learn Why](#)). Apps also have access to your friends list and any information you choose to make public.

### Apps you use

#### Platform is on.

Close

If you turn Platform off you can't use the Facebook integrations on third party apps or websites. If you want to use these apps and websites with Facebook, turn Platform back on. Using Platform allows you to bring your Facebook experience to the other apps and websites you use on the web and to your mobile device and apps. It allows Facebook to receive information about your use of third party apps and websites to provide you with better and more customized experiences. [Learn more](#).

If you turn off Platform apps:

- You will not be able to log into websites or applications using Facebook.
- Your friends won't be able to interact and share with you using apps and websites.
- Instant personalization will also be turned off.
- Apps you've previously installed may still have info you shared. Please contact these apps for details on removing this data.

Turn Off Platform

New Myspace

Public

Edit

### Apps others use

People who can see your info can bring it with them when they use apps. Use this setting to control the categories of information people can bring with them.

Edit

201. Only after a user had clicked “Turn Off Platform” would the user have prevented all access to her information from third-party app developers. This would have taken five affirmative clicks from the user.

202. Overall, this process exceeds the reasonable expectations of a user. Users who chose to limit their Privacy Settings to “friends,” “friends of friends,” and “public” would still have potentially shared their information with their friends’ apps developers.

203. Indeed, an FTC complaint from 2011 filed against Facebook outlines many of the same issues that have continued to persist throughout Graph API v1.0:

14. None of the pages . . . have disclosed that a user’s choice to restrict profile information to “Only Friends” or “Friends of Friends” would be ineffective as to certain third parties. Despite this fact, in many instances, Facebook has made profile information that a user chose to restrict to “Only Friends” or “Friends of Friends” accessible to any Platform Applications that the user’s Friends have used (hereinafter “Friends’ Apps”). Information shared with such Friends’ Apps has included, among other things, a user’s birthday, hometown, activities, interests, status updates, marital status, education (*e.g.*, schools attended), place of employment, photos, and videos.

15. Facebook’s Central Privacy Page and Profile Privacy Page have included links to “Applications,” “Apps,” or “Applications and Websites” that, when clicked, have taken users to a page containing “Friends’ App Settings,” which would allow users to restrict the information that their Friends’ Apps could access”

16. *However, in many instances, the links to “Applications,” “Apps,” or “Applications and Websites” have failed to disclose that a user’s choices made through Profile Privacy Settings have been ineffective against Friends’ Apps. For example, the language alongside the Applications link . . . has stated, “[c]ontrol what information is available to applications **you use** on Facebook.” (Emphasis added). Thus, users who did not themselves use applications would have had no reason to click on this link, and would have concluded that their choices to restrict profile information through their Profile Privacy Settings were complete and effective.*<sup>48</sup>

204. Moreover, this process required users to navigate through multiple webpages and privacy setting controls. By hiding the controls and establishing privacy settings that allowed sharing, Facebook sought to manufacture users’ consent.

### **3. Facebook Maintained the “Apps Others Use” Control Panel Until April 2018, Following the Cambridge Analytica Scandal**

205. Facebook has claimed that after it had phased out Graph API v1.0, app developers could no longer access friends’ data in the way GSR had done. Still, Facebook continued to keep the “Apps Others Use” control panel on users’ Apps Settings webpage until as late as March 2018.<sup>49</sup>

206. On March 22, 2018, CNET reported the following controls were still set to be automatically shared with third parties:<sup>50</sup>

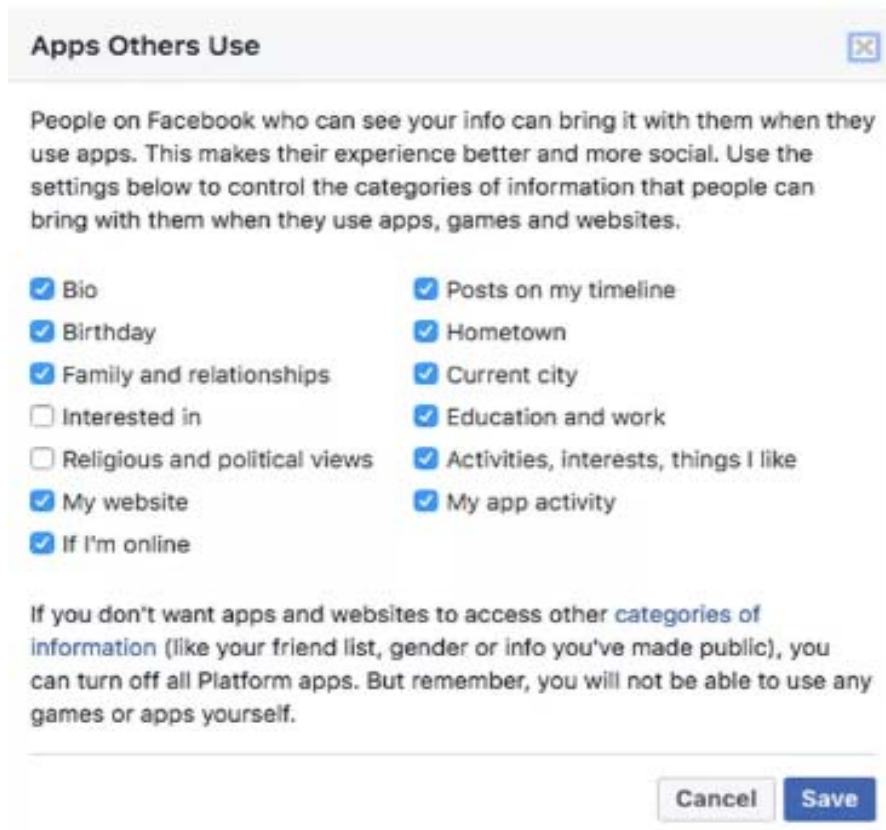
---

<sup>48</sup> FTC Complaint, *In re Facebook, Inc.*, No. C-4365 (F.T.C. July 2012), <https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookcmpt.pdf> (emphasis added).

<sup>49</sup> Brian Barrett, *The Facebook Privacy Setting That Doesn’t Do Anything at All*, Wired (Mar. 27, 2018), <https://www.wired.com/story/facebook-privacy-setting-doesnt-do-anything>.

<sup>50</sup> Laura Hautala, *Facebook Privacy Settings Make You Work to Stop the Data Sharing*, CNET (Mar. 22, 2018), <https://www.cnet.com/news/how-to-stop-sharing-facebook-data-after-cambridge-analytica-mess>.





207. This display contained 11 distinct categories of information set to automatically be shared with third parties through the users' friends. This display also contained the same disclosures as the display active during API v1.0.

208. Facebook maintains that after Graph API v1.0, developers could no longer access friends' data unless each friend had "explicitly granted permission to the developer[s]."<sup>51</sup> Yet, Facebook has identified at least one category of information, "[p]osts on my timeline," that if checked, allowed app developers to access a photo or video that a friend uploaded if the user had allowed tagged photos of herself to show up on the downloading users' timeline.<sup>52</sup>

<sup>51</sup> Brian Barrett, *The Facebook Privacy Setting That Doesn't Do Anything at All*, Wired (Mar. 27, 2018), <https://www.wired.com/story/facebook-privacy-setting-doesnt-do-anything>.

<sup>52</sup> *Id.* ("I can't really make any sense of it, actually," says [Professor Gergely Biczok of Budapest University of Technology and Economics's CrySys Lab], who says that the data categories in the settings pane line up essentially one-for-one with a permission called friends\_XXX, which allowed developers to harvest friend data, and which Facebook says was phased out with the advent of Graph API v2.0 in 2014. 'Even if I do a thought experiment and try to imagine myself into their place, it's maybe just an error in the software development process. But it's a long-existing one.'").

209. Moreover, the “read\_mailbox” category of information, available originally under Graph API v1.0, was only removed in Graph API v2.4, which was introduced on July 8, 2015.<sup>53</sup> Through this category, developers were able to read the private messages between the downloading user and her friends. This category raises significant privacy concerns.

210. Even accepting as true Facebook’s claim that access to this category of information did not last beyond Graph API v.1.0, its presence in Graph API v.1.0 shows a disregard for the controls users have access to.

**D. In the Documents That Purport to Govern the Relationship Between Facebook and Its Users, Facebook Made Promises About Privacy That It Broke, and Also Failed to Properly Disclose the Access to Users’ Content and Information That It Gave to Third Parties.**

211. To support the notion that users consented to the disclosures of data that are the subject of this action, Facebook has pointed to a number of different documents. In this section, Plaintiffs will explain in detail what these documents were, where they were to be found, and what they did and did not say.

212. One of these documents is the Statement of Rights and Responsibilities, which before 2009 was called the Terms of Use. This was the document that constituted the contract between Facebook and its users. Facebook’s conduct violated one of the key promises it made in that document.

213. Another important document is Facebook’s Data Use Policy, which at times has also gone by the names “Data Policy” or “Privacy Policy.” This document, as Plaintiffs will explain, was *not* part of the contract between Facebook and its users.

214. What is more, Facebook has kept the Data Use Policy consistently difficult for users to access. And even if users *did* access it, it failed to meaningfully disclose how Facebook allowed third parties access to users’ content and information, and what Facebook enabled them to do with that content and information.

215. On top of those sources of confusion, both the Statement of Rights and

---

<sup>53</sup> *Id.*; *Facebook for Developers: Changelog*, Facebook, <https://developers.facebook.com/docs/graph-api/changelog/archive> (last visited Sept. 20, 2018).

Responsibilities and the Data Use Policy were constantly being amended. And they were consistently amended *without* notice to users.

# **1. What the Statement of Rights and Responsibilities Promised**

216. A Facebook user could access the operative Statement of Rights and Responsibilities—the contract between Facebook and its Users—by clicking the “Terms” hyperlink located at the bottom of Facebook’s landing page. For example:



217. The visual presentation of the Statements of Rights and Responsibilities remained substantially the same throughout the Class Period. The top of the page containing the Statement of Rights and Responsibilities appeared as follows.

facebook	Email	Password	Login
	<input type="text"/>	<input type="text"/>	
	<input type="checkbox"/> Keep me logged in	Forgot your password?	

This agreement was written in English (US). To the extent any translated version of this agreement conflicts with the English version, the English version controls. Please note that Section 16 contains certain changes to the general terms for users outside the United States.

Date of Last Revision: October 4, 2010.

#### Statement of Rights and Responsibilities

This Statement of Rights and Responsibilities ("Statement") derives from the Facebook Principles, and governs our relationship with users and others who interact with Facebook. By using or accessing Facebook, you agree to this Statement.

##### 1. Privacy

Your privacy is very important to us. We designed our Privacy Policy to make important disclosures about how you can use Facebook to share with others and how we collect and can use your content and information. We encourage you to read the Privacy Policy, and to use it to help make informed decisions.

##### 2. Sharing Your Content and Information

You own all of the content and information you post on Facebook, and you can control how it is shared through your privacy and application settings. In addition:

1. For content that is covered by intellectual property rights, like photos and videos ("IP content"), you specifically give us the following permission, subject to your privacy and application settings: you grant us a non-exclusive, transferable, sub-licensable, royalty-free, worldwide license to use any IP content that you post on or in connection with Facebook ("IP License"). This IP License ends when you delete your IP content or your account unless your content has been shared with others, and they have not deleted it.
2. When you delete IP content, it is deleted in a manner similar to emptying the recycle bin on a computer. However, you understand that removed content may persist in backup copies for a reasonable period of time (but will not be available to others).
3. When you use an application, your content and information is shared with the application. We require applications to respect your privacy, and your agreement with that application will control how the application can use, store, and transfer that content and information. (To learn more about Platform, read our Privacy Policy and Platform Page.)
4. When you publish content or information using the "everyone" setting, it means that you are allowing everyone, including people off of Facebook, to access and use that information, and to associate it with you (i.e., your name and profile picture).
5. We always appreciate your feedback or other suggestions about Facebook, but you understand that we may use them without any obligation to compensate you for them (just as you have no obligation to offer them).

##### 3. Safety

We do our best to keep Facebook safe, but we cannot guarantee it. We need your help to do that, which includes the following commitments:

1. You will not send or otherwise post unauthorized commercial communications (such as spam) on Facebook.
2. You will not collect users' content or information, or otherwise access Facebook, using automated means (such as harvesting bots, robots, spiders, or scrapers) without our permission.
3. You will not engage in unlawful multi-level marketing, such as a pyramid scheme, on Facebook.
4. You will not upload viruses or other malicious code.
5. You will not solicit login information or access an account belonging to someone else.
6. You will not bully, intimidate, or harass any user.
7. You will not post content that is hateful, threatening, or pornographic; incites violence; or contains nudity or graphic or gratuitous violence.
8. You will not develop or operate a third-party application containing alcohol-related or other mature content (including advertisements) without appropriate age-based restrictions.
9. You will not offer any contest, giveaway, or sweepstakes ("promotion") on Facebook without our prior written consent. If we consent, you take full responsibility for the promotion, and will follow our Promotions Guidelines and all applicable laws.
10. You will not use Facebook to do anything unlawful, misleading, malicious, or discriminatory.
11. You will not do anything that could disable, overburden, or impair the proper working of Facebook, such as a denial of service attack.
12. You will not facilitate or encourage any violations of this Statement.

#### a. The Statement of Rights and Responsibilities Promised to Respect Users' Privacy

218. The second section of the Statement of Rights and Responsibilities is titled "Sharing Your Content and Information." While the text of this section changed numerous times, no version of this provision notifies users of the amount of information third parties could access via a users' friends. Moreover, Facebook notified users of these changes just once, in 2014.<sup>54</sup>

219. From May 1, 2009 to August 28, 2009, this section read:

You own all of the content and information you post on Facebook, and you can control how it is shared through your privacy [hyperlinked] and application [hyperlinked] settings. In order for us to use certain types of content and provide you with Facebook, you

<sup>54</sup> Steve Kovach, *Facebook's Privacy Policy Is Changing And You're Going To Get A Long Email About It*, Bus. Insider (Nov. 27, 2014), <https://www.businessinsider.com/facebook-privacy-policy-change-2014-11>.

agree to the following . . .

However, none of the following three paragraphs described data collection from third parties. Facebook at all relevant times stated in its Statement of Rights and Responsibilities and elsewhere that Plaintiffs and Class Members owned and controlled their content and information. This was a property right defined by the contract itself and these terms applied throughout the Class Period.

220. From August 28, 2009 to April 22, 2010, the following paragraph was added to this section:

When you add an application and use Platform, your content and information is shared with the application. We require applications to respect your privacy settings, but your agreement with that application will control how the application can use the content and information you share. (To learn more about Platform, read our About Platform [hyperlinked] page.)<sup>55</sup>

221. On April 22, 2010, Facebook revised this Content and Information provision as follows:

When you add an application and use Platform, your content and information is shared with the application. We require applications to respect your privacy ~~settings~~, but and your agreement with that application will control how the application can use, store, and transfer that the content and information ~~you share~~. (To learn more about Platform, read our Privacy Policy [hyperlinked] and About Platform page [hyperlinked].)<sup>56</sup>

222. On June 8, 2012, Facebook changed the Content and Information provision as follows:

When you use an application, the application may ask for your permission to access your content and information ~~is shared with the application as well as content and information that others have shared with you~~. We require applications to respect your privacy, and

---

<sup>55</sup> *Statement of Rights and Responsibilities*, Facebook (Aug. 28, 2009), <https://www.facebook.com/terms.php> [<https://web.archive.org/web/20091220022337/facebook.com/terms.php>]. This policy also defines “information” as “facts and other information about you, including actions you take.” *Id.* And it defines “content” as “anything you post on Facebook that would not be included in the definition of ‘information.’” *Id.*

<sup>56</sup> *Statement of Rights and Responsibilities*, Facebook (Apr. 22, 2010), <https://www.facebook.com/terms.php> [<https://web.archive.org/web/20100807133449/https://www.facebook.com/terms.php>].

your agreement with that application will control how the application can use, store, and transfer that content and information. (To learn more about Platform, read our [Data Use Policy](#) [hyperlinked] and Platform Page [hyperlinked].)<sup>57</sup>

This version remained in place until April 2018.

223. The terms “information” and “content” are used in each version of this provision. Facebook defined these terms in Section 17 of 18 of the Statement of Rights and Responsibilities and it changed the definitions of these terms over time. The May 1, 2009 Statement of Rights and Responsibilities defined “content” as “the content and information you post on Facebook, including information about you and the actions you take.”<sup>58</sup> Starting with the August 28, 2009 Statement of Rights and Responsibilities, Facebook defined “information” as “facts and other information about you, including actions you take”<sup>59</sup>; before the August 28, 2009 Statement of Rights and Responsibilities, “information” remained undefined. Facebook defined “content” as “anything you post on Facebook that would not be included in the definition of ‘information.’”<sup>60</sup>

224. On June 8, 2012, Facebook broadened these definitions. “Information” was newly defined as “facts and other information about you, including *actions taken by users and non-users who interact with Facebook*” (emphasis added to show addition).<sup>61</sup> The new definition of “content” was “anything you *or other users* post on Facebook that would not be included in the

---

<sup>57</sup> *Statement of Rights and Responsibilities*, Facebook (June 8, 2012), <https://www.facebook.com/legal/terms> [<https://web.archive.org/web/20121205191915/https://www.facebook.com/legal/terms>] (emphasis added) (red and underlined text shows newly added text and strikethrough text shows newly deleted text).

<sup>58</sup> *Statement of Rights and Responsibilities*, Facebook (May 1, 2009), <http://www.facebook.com/terms.php> [<https://web.archive.org/web/20090826051726/facebook.com/terms.php>].

<sup>59</sup> *Statement of Rights and Responsibilities*, Facebook (Aug. 28, 2009), <http://www.facebook.com/terms.php> [<https://web.archive.org/web/20091220022337/facebook.com/terms.php>].

<sup>60</sup> *Id.*

<sup>61</sup> *Statement of Rights and Responsibilities*, Facebook (June 8, 2012), <https://www.facebook.com/legal/terms> [<https://web.archive.org/web/20121205191915/https://www.facebook.com/legal/terms>].

definition of information.”<sup>62</sup> Facebook unhelpfully attempted to explain:

[Facebook] updated this language to be clearer and consistent with what has long been reflected in our Data Use Policy and our practices—that when you, or friends you have authorized to see your information, use an App, you are sharing your info with that App, which is what you consented to when you installed the App.”<sup>63</sup>

225. In this section, Facebook also promised users that even though a user’s content and information was shared with an application when the application was used, Facebook “require[d] applications to respect your privacy.” Yet Facebook did not audit applications’ treatment of users’ content and information. For example, Facebook is still unable to identify who possesses the content and information taken by Cambridge Analytica.

226. Nowhere in the operative contracts did Facebook disclose to users that device makers, mobile carriers, software makers, security firms or chip designers would have access to their content and information notwithstanding their privacy settings.

**b. The Statement of Rights and Responsibilities Promised Users Throughout the Class Period That Facebook Would Not Share Content or Information With Advertisers Without Their Consent**

227. The May 1, 2009 Statement of Rights and Responsibilities includes the following language:

Our goal is to deliver ads that are not only valuable to advertisers, but also valuable to you. In order to do that, you agree to the following:

1. You can use your privacy [hyperlinked] settings to limit how your name and profile picture may be associated with commercial or sponsored content. You give

---

<sup>62</sup> *Statement of Rights and Responsibilities*, Facebook (June 8, 2012), <https://www.facebook.com/legal/terms> [<https://web.archive.org/web/20121205191915/https://www.facebook.com/legal/terms>] (As noted in the Introduction, this complaint uses “content and information” as Facebook’s Statement of Rights and Responsibilities have defined those two terms. When this complaint uses “content and information” in regard to a particular time, it incorporates the meaning of “content” and “information” as defined by the Statement of Rights and Responsibilities that was operative at that time.).

<sup>63</sup> Jamillah Knowles, *Facebook Updates Statement of Rights and Responsibilities, You Have Until March 22 to Respond*, Next Web (Mar. 18, 2012), <https://thenextweb.com/facebook/2012/03/18/facebook-updates-statement-of-rights-and-responsibilities-you-have-until-march-22-to-respond/>.



us permission to use your name and profile picture in connection with that content, subject to the limits you place.

2. We do not give your content to advertisers.

228. In the August 28, 2009 Statement of Rights and Responsibilities, this language was changed as follows:

Our goal is to deliver ads that are not only valuable to advertisers, but also valuable to you. In order to do that, you agree to the following:

1. You can use your privacy [hyperlinked] settings to limit how your name and profile picture may be associated with commercial or sponsored content served by us. You give us permission to use your name and profile picture in connection with that content, subject to the limits you place.

2. We do not give your content or information to advertisers without your consent.

229. Then, in the October 4, 2010 Statement of Rights and Responsibilities, this language was changed as follows:

Our goal is to deliver ads that are not only valuable to advertisers, but also valuable to you. In order to do that, you agree to the following:

1. You can use your privacy settings [hyperlinked] to limit how your name and profile picture may be associated with commercial, sponsored, or related content (such as brand you like) served or enhanced by us. You give us permission to use your name and profile picture in connection with that content, subject to the limits you place.

2. We do not give your content or information to advertisers without your consent.

230. Next, in the June 8, 2012 Statement of Rights and Responsibilities, the language was changed to state:

Our goal is to deliver ads and commercial content that are valuable to users and advertisers []. In order to help us do that, you agree to the following:

1. You can use your privacy settings [hyperlinked] to limit how your name and profile picture may be associated with commercial, sponsored, or related content (such as brand you like) served or enhanced by us. You give us permission to use your name and profile picture in connection with that content, subject to the limits you place.



2. We do not give your content or information to advertisers without your consent.

231. This statement falsely claimed that users could control what Facebook shared with third parties through their privacy settings. However, a user's privacy settings would not have necessarily prevented an app developer from obtained information through that user's friends.

232. In the November 15, 2013 Statement of Rights and Responsibilities this language was changed to read:

Our goal is to deliver **advertising** and **other** commercial **or sponsored** content that **is** valuable to **our** users and advertisers. In order to help us do that, you agree to the following:

1. You **give us permission to use** your name, profile picture, **content, and information in connection with** commercial, sponsored, or related content (such as brand you like) served or enhanced by us. **This means, for example, that you permit a business or other entity to pay us to display your name and/or profile picture with your content or information, without compensation to you. If you have selected a specific audience for your content or information, we will respect your choice when we use it.**

2. We do not give your content or information to advertisers without your consent.

233. The language remains unaltered in the subsequent Statement of Rights and Responsibilities published on January 30, 2015.

234. Facebook's promise not to give your content or information to advertisers without your consent is also false. In order to limit what a third-party app developer could have obtained on Graph API v1.0, a user would have had to affirmatively change their "app settings."

**c. The Statement of Rights and Responsibilities Promised to Adequately Notify Users When It Was Amended**

235. Facebook did not adequately notify its users when it updated the Statement of Rights and Responsibilities. From 2005 to 2018 this policy changed over twenty times.

236. On May 1, 2009, the Amendments section of the Statement of Rights and

Responsibilities stated the following:<sup>64</sup>

1. “We can change this Statement so long as we provide you notice through Facebook (unless you opt-out of such notice) and an opportunity to comment.”

2. For changes to sections 7, 8, 9, and 11 (sections relating to payments, application developers, website operators, and advertisers), we will give you minimum of three days notice. For all other changes we will give you a minimum of seven days notice. Comments to proposed changes will be made on the Facebook Site Governance Page [hyperlink].

3. If more than 7,000 users post a substantive comment on a particular proposed change, we will also give you the opportunity to participate in a vote in which you will be provided alternatives. The vote shall be binding on us if more than 30% of all active registered users as of the date of the notice vote.

4. We can make changes for legal or administrative reasons, or to correct an inaccurate statement, upon notice without opportunity to comment.

237. On August 28, 2009 the first paragraph of this section changed to the following:<sup>65</sup>

1. We can change this Statement **if we provide you notice (by posting the change on the Facebook Site Governance Page [hyperlink]) and an opportunity to comment. To get notice of any future changes to this Statement, visit our Facebook Site Governance Page [hyperlink] and become a fan**

However, paragraphs two through four were not altered.

238. On June 8, 2012, two paragraphs were added to the Amendments section. This section now read:<sup>66</sup>

1: We can change this Statement if we provide you notice (by posting the change on the Facebook Site Governance Page [hyperlink]) and an opportunity to comment. To get notice of any future changes to this Statement, visit our Facebook Site Governance Page [hyperlink] and become a fan.”

---

<sup>64</sup> *Statement of Rights and Responsibilities*, Facebook (May 1, 2009), <http://www.facebook.com/terms.php> [<https://web.archive.org/web/20090826051726/facebook.com/terms.php>].

<sup>65</sup> *Statement of Rights and Responsibilities*, Facebook (Aug. 28, 2009), <https://www.facebook.com/terms.php> [<https://web.archive.org/web/20091220022337/facebook.com/terms.php>].

<sup>66</sup> *Statement of Rights and Responsibilities*, Facebook (June 8, 2012), <https://www.facebook.com/legal/terms> [<https://web.archive.org/web/20121205191915/https://www.facebook.com/legal/terms>].

2: For changes to sections 7, 8, 9, and 11 (sections relating to payments, application developers, website operators, and advertisers), we will give you minimum of three days notice. For all other changes we will give you a minimum of seven days notice. Comments to proposed changes will be made on the Facebook Site Governance Page [hyperlink].

3: If more than 7,000 users post a substantive comment on a particular proposed change, we will also give you the opportunity to participate in a vote in which you will be provided alternatives. The vote shall be binding on us if more than 30% of all active registered users as of the date of the notice vote.

4. If we make changes to policies referenced in or incorporated by this Statement, we may provide notice on the Site Governance Page.

5. We can make changes for legal or administrative reasons, or to correct an inaccurate statement, upon notice without opportunity to comment.

6. Your continued use of Facebook following changes to our terms constitutes your acceptance of our amended terms.

239. This section changed entirely on December 11, 2012 to including only the following three paragraphs:<sup>67</sup>

1. Unless we make a change for legal or administrative reasons, or to correct an inaccurate statement, we will provide you with seven (7) days notice (for example, by posting the change on the Facebook Site Governance Page [hyperlink]) and an opportunity to comment. You can also visit our Facebook Site Governance Page [hyperlink] and “like” the Page to get update about changes to this statement.

2. If we make changes to the policies referenced in or incorporated by this statement, we may provide notice on the Site Governance Page.

3. Your continued use of Facebook following changes to our terms constitutes your acceptance of our amended terms.”

240. On January 30, 2015, this section changed again to read:<sup>68</sup>

---

<sup>67</sup> *Statement of Rights and Responsibilities*, Facebook (Dec. 11, 2012), <https://www.facebook.com/legal/terms> [<https://web.archive.org/web/20131024211134/https://www.facebook.com/legal/terms>].

<sup>68</sup> *Statement of Rights and Responsibilities*, Facebook (Jan. 30, 2015), <https://www.facebook.com/legal/terms> [<https://web.archive.org/web/20150130004354/https://www.facebook.com/legal/terms>].

1. We'll notify you before we make changes to these terms and give you the opportunity to review and comment on the revised terms before continuing to use our Services.

2. If we make changes to policies, guidelines or other terms referenced in or incorporated by this Statement, we may provide notice on the Site Governance Page.

3. Your continued use of the Facebook Services, following notice of the changes to our terms, policies or guidelines, constitutes your acceptance of our amended terms, policies or guidelines.”

**2. The Statement of Rights and Responsibilities Did Not Incorporate or Make Binding Facebook's Other Policies**

241. Facebook may claim that documents other than the Statement of Rights and Responsibilities were part of the contracts between Facebook and its users. That claim is wrong, as Plaintiffs will now explain.

242. The Statement of Rights and Responsibilities contained a “Privacy” section. This section was a mere three sentences that “encourage[d],” but in no way required, a user to read or consent to Facebook's separate Privacy Policy.<sup>69</sup>

243. At all relevant times until June 8, 2012, the second paragraph of the Statement of Rights and Responsibilities, titled “Privacy,” read as follows:

Your privacy is very important to us. We designed our Privacy Policy [hyperlinked] to make important disclosures about how you can use Facebook to share with others and how we collect and can use your content and information. We encourage you to read the Privacy Policy, and to use it to help make informed decisions.<sup>70</sup>

244. After June 8, 2012, Facebook changed the “Privacy” section of the Statement of Rights and Responsibilities to refer to the newly named “Data Use Policy.” This change in name is significant and purposeful. A user is likely to think a Privacy Policy contains relevant information to his or her information. “Data Use Policy,” by contrast, does not carry the same

---

<sup>69</sup> The “Privacy Policy” was relabeled to “Date Policy” on June 8, 2012 and relabeled again to “Data Use Policy” on December 11, 2012.

<sup>70</sup> *Data Policy*, Facebook (Dec. 9, 2009), [facebook.com/policy.php](https://web.archive.org/web/20100402021414/facebook.com/policy.php) [<https://web.archive.org/web/20100402021414/facebook.com/policy.php>].

associations. The new section read:

Your privacy is very important to us. We designed our ~~Privacy Policy~~ **Data Use Policy** [hyperlinked] to make important disclosures about how you can use Facebook to share with others and how we collect and can use your content and information. We encourage you to read the ~~Privacy Policy~~ **Data Use Policy**, and to use it to help make informed decisions.<sup>71</sup>

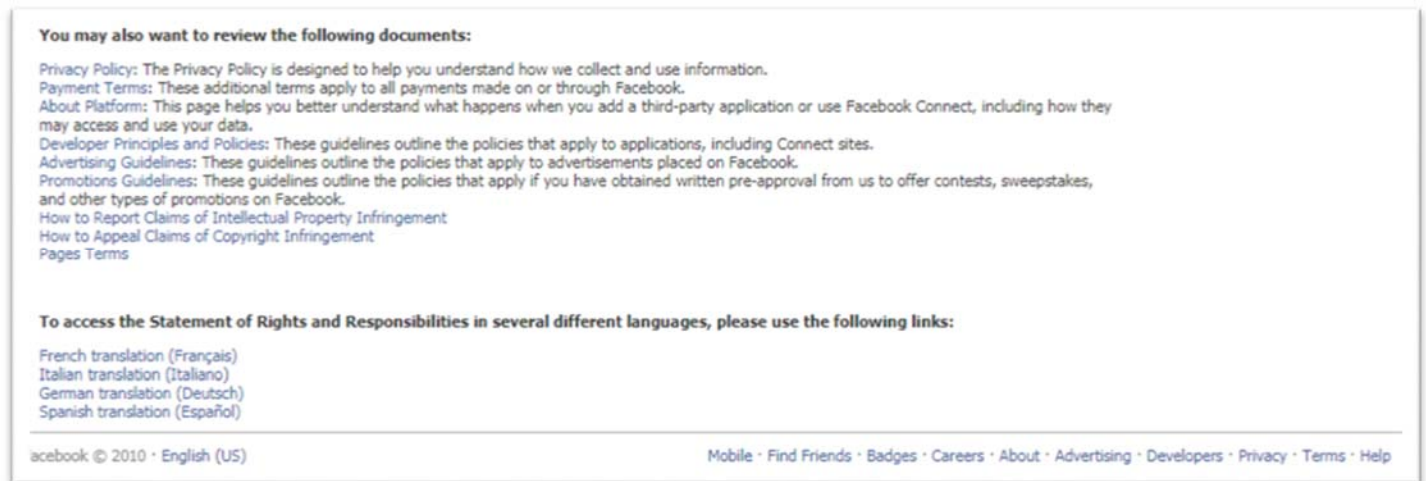
245. Notably, the Statement of Rights and Responsibilities did not contain the full text of either the Privacy Policy or the Data Use Policy. The Statement of Rights and Responsibilities did not require users to review either Policy, let alone read them carefully. Nor did the Statement of Rights and Responsibilities require any form of affirmative acknowledgement of or consent to the Privacy Policy or Data Use Policy—all despite the fact these Policies contained “important disclosures” about Facebook’s collection and use of users’ “content and information.”

246. Finally, at the bottom of the Statement of Rights and Responsibilities, the privacy policy was hyperlinked in a long list of documents that Facebook casually suggested users “may also want to review.” Facebook explained in this list that the “Privacy Policy is designed to help you understand how [they] collect and use information”—in other words, it was a help page, *not* an agreement, and certainly not up for negotiation. Facebook failed to specify here exactly what “information” it was collecting and using, or how; users had to click through to the Privacy Policy to find out. Once again, there was no requirement to consent to the Privacy Policy before using Facebook, nor did Facebook require any affirmative consent to the policy from a user. A

---

<sup>71</sup> *Data Policy*, Facebook (Apr. 22, 2010), <http://www.facebook.com/policy.php> [<https://web.archive.org/web/20100923040926/http://www.facebook.com/policy.php>].

typical example of this portion of the Statement of Rights and Responsibilities follows:<sup>72</sup>



### 3. Facebook’s “Policies” Were Generally Difficult to Access, Confusing, and Constantly Changing Without Notice.

#### a. To Access the Contents of the Privacy, the Data Use, and Data Policies, Users Were Forced to Navigate a Maze of Hyperlinks

247. Like the Terms of Use and later the Statement of Rights and Responsibilities, Facebook provided a hyperlink to the Privacy and Data Use Policy on its home screen. This link was clearly distinguished as “Privacy” on Facebook’s launching screen.

248. Prior to September 2011, if a curious user clicked on this hyperlink, she would be routed to one webpage that contained the entire Policy as shown by the December 22, 2010 screenshot below:

<sup>72</sup> *Id.*; *Statement of Rights and Responsibilities*, Facebook (June 18, 2010), <http://www.facebook.com/terms.php?ref=pf> [<https://web.archive.org/web/20100618213653/http://www.facebook.com/terms.php?ref=pf>].

**Facebook's Privacy Policy.**

Date of last revision: December 22, 2010.

This policy contains nine sections, and you can jump to each by selecting the links below:

1. Introduction
2. Information We Receive
3. Sharing information on Facebook
4. Information You Share With Third Parties
5. How We Use Your Information
6. How We Share Information
7. How You Can Change or Remove Information
8. How We Protect Information
9. Other Terms

**1. Introduction**

**Questions.** If you have any questions or concerns about our privacy policy, contact our privacy team through this [help page](#). You may also contact us by mail at 1601 S. California Avenue, Palo Alto, CA 94304.

**TRUSTe Program.** Facebook has been awarded TRUSTe's Privacy Seal signifying that this privacy policy and practices have been reviewed by TRUSTe for compliance with TRUSTe's program requirements. If you have questions or complaints regarding our privacy policy or practices, please contact us by mail at 1601 S. California Avenue, Palo Alto, CA 94304 or through this [help page](#). If you are not satisfied with our response you can contact TRUSTe [here](#). This privacy policy covers the website [www.facebook.com](#). The TRUSTe program covers only information that is collected through this Web site, and does not cover other information, such as information that may be collected through software downloaded from Facebook.

**TRUSTe****TO VERIFY**

**Safe Harbor.** Facebook also complies with the EU Safe Harbor framework as set forth by the Department of Commerce regarding the collection, use, and retention of data from the European Union. As part of our participation in the Safe Harbor, we agree to resolve all disputes you have with us in connection with our policies and practices through TRUSTe. We will also provide initial responses to access requests within a reasonable period of time. To view our certification, visit the U.S. Department of Commerce's [Safe Harbor Web site](#).

**Scope.** This privacy policy covers all of Facebook. It does not, however, apply to entities that Facebook does not own or control, such as applications and websites using Platform. By using or accessing Facebook, you agree to our privacy practices outlined [here](#).

**No information from children under age 13.** If you are under age 13, please do not attempt to register for Facebook or provide any personal information about yourself to us. If we learn that we have collected personal information from a child under age 13, we will delete that information as quickly as possible. If you believe that we might have any information from a child under age 13, please contact us through this [help page](#).

**Parental participation.** We strongly recommend that minors 13 years of age or older ask their parents for permission before sending any information about themselves to anyone over the Internet and we encourage parents to teach their children about safe Internet use practices. Materials to help parents talk to their children about safe Internet use can be found on this [help](#)

249. Facebook changed this process starting at least by September 2011. Thereafter, if a user clicked the “privacy” hyperlink she would be routed to a different landing page that listed subheadings of the “Data Use Policy”. For example, from the September 7, 2011 policy:<sup>73</sup>

<sup>73</sup> *Data Use Policy*, Facebook (Sept. 7, 2011), <http://www.facebook.com/about/privacy/your-info-on-other> [<https://web.archive.org/web/20110922202503/http://www.facebook.com/about/privacy/your-info-on-other>].



facebook

Email  Password

☐ Keep me logged in [Forgot your password?](#)

Facebook helps you connect and share with the people in your life.

---

## Data Use Policy

Last updated: September 23, 2011

### Information we receive and how it is used

Learn about the types of information we receive, and how that information is used.

### Sharing and finding you on Facebook

Get to know the privacy settings that help you control your information on facebook.com.

### Sharing with other websites and applications

Find out about the ways your information is shared with the games, applications and websites you and your friends use off Facebook.

### How advertising works

See how ads are served without sharing your information with advertisers, and understand how we pair ads with social context, such as newsfeed-style stories.

### Minors and Safety

Find out how Facebook protects minors, and what you can do to protect yourself and others online.

### Some other things you need to know

Learn how we make changes to this policy and more.

If you have questions or complaints regarding our privacy policy or practices, please contact us by mail at 1601 S. California Avenue, Palo Alto, CA 94304 or through this [help page](#).

More resources

**Interactive Tools**

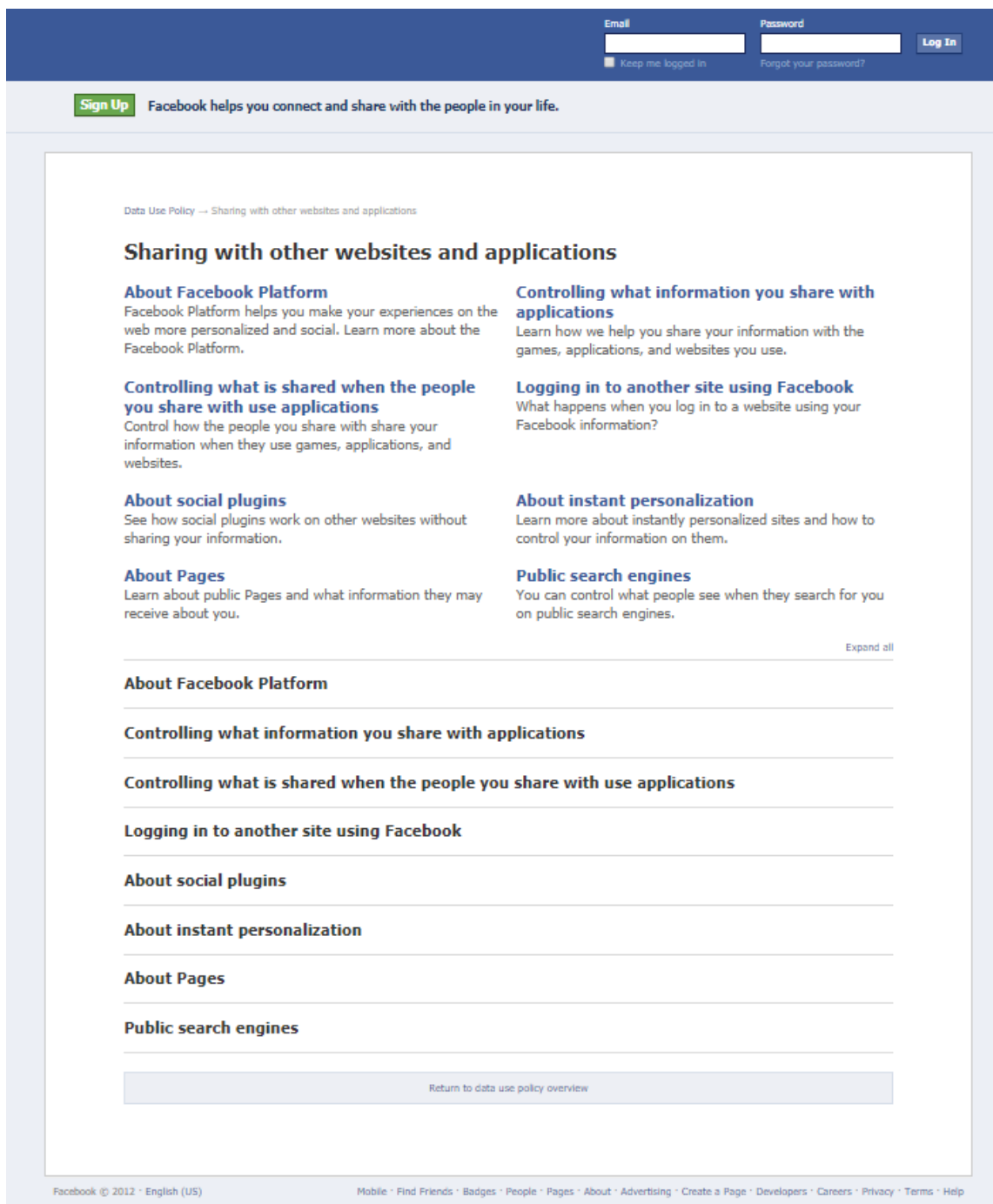
[View the complete Data Use Policy](#)

Facebook © 2011 • English (US)      Mobile • Find Friends • Badges • People • Pages • About • Advertising • Create a Page • Developers • Careers • Privacy • Terms • Help

250. From September 2011 to June 2012, if users clicked a subheading on this webpage, they still would not be able to see the contents of the Data Use Policy. Instead, clicking those subheadings routed users to yet another webpage containing yet more subheadings. Users would then need to read and click on the subheadings or click “*expand all*” to actually read the content of the relevant subsection of the Data Use Policy. For example, if users decided they wanted to read more about “Sharing with other websites and applications,” they would be routed to the following screen:<sup>74</sup>

<sup>74</sup> *Sharing with other websites and applications*, Facebook (Jan. 12, 2012), <http://www.facebook.com/about/privacy/your-info-on-other> [<https://web.archive.org/web/20120112084445/http://www.facebook.com/about/privacy/your-info-on-other>].



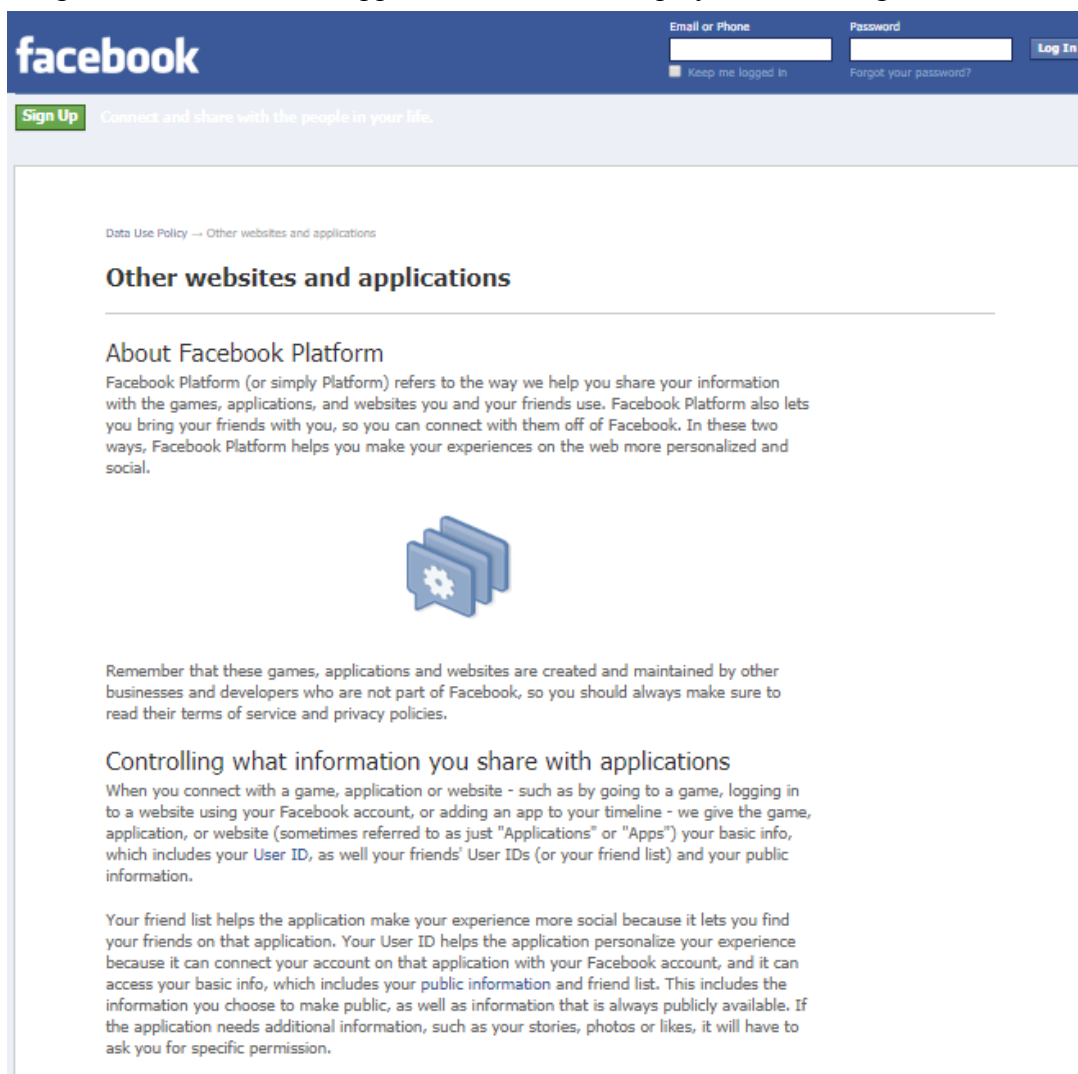


251. As shown above, this webpage required users to read still *more* subheadings before accessing the actual content of the “Data Use Policy.”

252. Thus, from September 2011 to June 2012, if a user wanted to read the actual contents of the Data Use Policy, the user would have had to read several subheading descriptions and to click at least three different hyperlinks before seeing any content. And, if the user wanted

to read the *full* Data Use Policy, the user would need to click back and forth between multiple webpages. It would take a user at least eighteen separate clicks of the mouse to read the entire Data Use Policy.

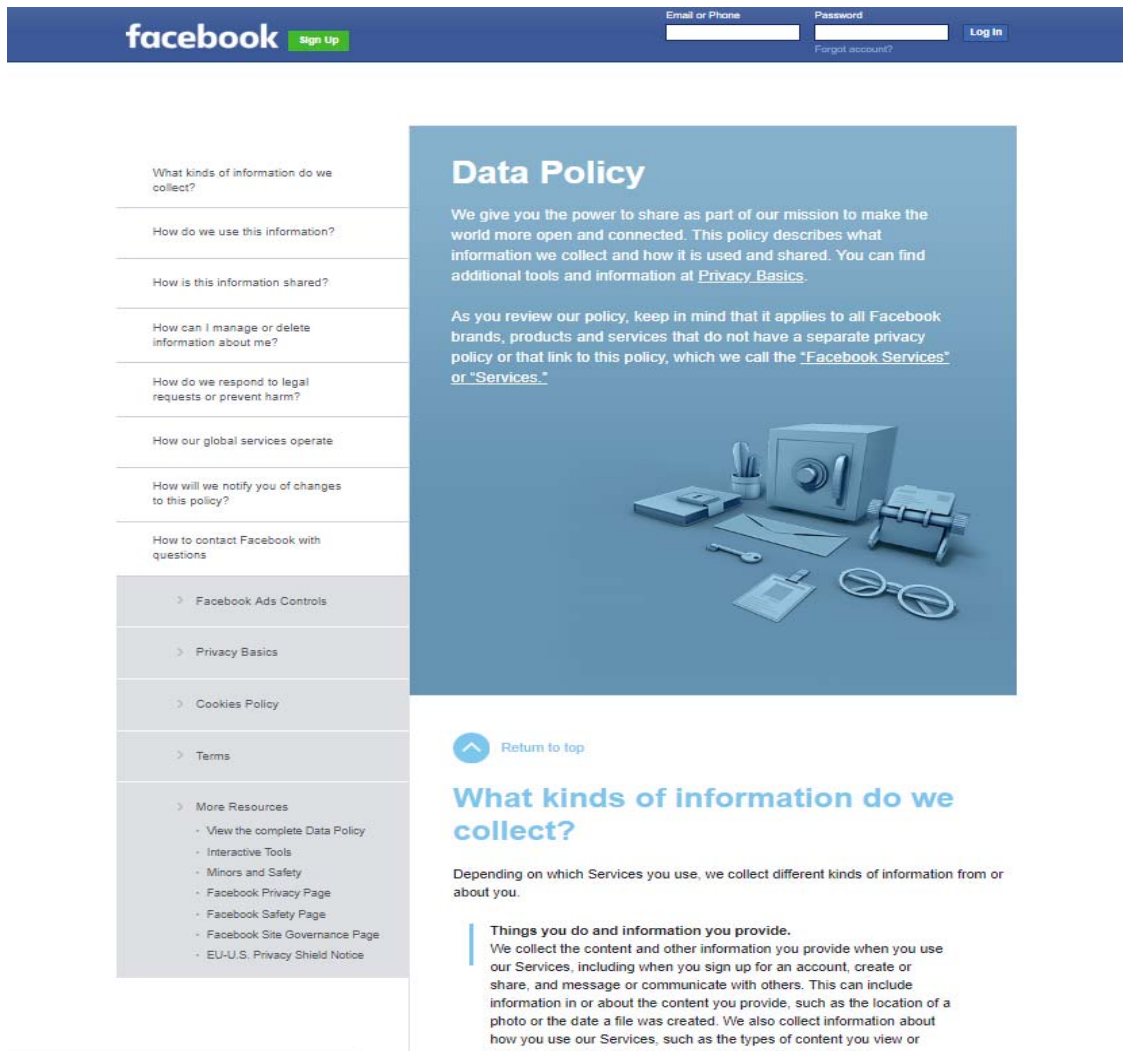
253. Even after June 2012, Facebook still required users to click on one of the six separate subheadings of the Data Use Policy, although beginning in June 2012, Facebook began displaying the actual contents of the Data Use Policy's subsections without requiring a user to further click on more subheadings or choose "*expand all*." For example, clicking on the subheading "Other websites and applications," would display the following:<sup>75</sup>



<sup>75</sup> *Other Website and Applications*, Facebook (Dec. 9, 2012), <https://www.facebook.com/about/privacy/your-info-on-other> [https://web.archive.org/web/20121209131947/https://www.facebook.com/about/privacy/your-info-on-other].

254. Even with this change, from June 2012 to January 2015, a user would need to click back and forth at least twelve times in order to read the full contents of the Data Use Policy contained within six separate subheadings.

255. Starting in January 2015, Facebook again changed the Data Use Policy so that all content was displayed on one webpage. A user would see the following:<sup>76</sup>



256. On this page, the headings on the left side—“What kinds of information do we collect?,” “How do we use this information?,” etc.—were hyperlinked to sections further down on the same page on each topic.

<sup>76</sup> *Data Policy*, Facebook (Oct. 18, 2016), <http://www.facebook.com/about/privacy> [<https://web.archive.org/web/20161018003814/www.facebook.com/about/privacy>].

**b. Users Often Were Not Required to Read the Contents of the Privacy, the Data Use, or Data Policies When They Signed Up**

257. Since its creation, Facebook has required little of users signing up for a new account.

258. From 2005 to March 2006, Facebook required new users to affirmatively click a box next to a statement. In 2005, that statement read, “I have read and understood the Terms of Use [hyperlinked], and I agree to them.”<sup>77</sup>

259. From March 2006 to May 2007, users had to affirmatively check a box next to a statement that said: “I have read and agree to the Terms of Use [hyperlinked].”<sup>78</sup> From May of 2007 to May 2008, users had to affirmatively check a box next to a statement that said: “I have read and agree to the Terms of Use [hyperlinked] and Privacy Policy [hyperlinked].”<sup>79</sup>

260. Beginning in May 2008, Facebook no longer required users to affirmatively check the box acknowledging the Terms of Use. Instead, next to the “Sign Up” link Facebook added a statement that read “By clicking Sign Up, you are indicating that you have read and agree to the Terms of Use [hyperlinked] and Privacy Policy [hyperlinked].”<sup>80</sup>

261. In March 2009, Facebook changed its registration process again by omitting any reference to the Statement of Rights and Responsibilities or the Privacy Policy on the initial registration page.<sup>81</sup> This initial screen required the user to complete the following fields: first name; last name; email; password; sex; and birthday. An example from 2011 is show below:

---

<sup>77</sup> *Facebook Registration*, Facebook (Oct. 4, 2005), <http://www.facebook.com/register.php> [<https://web.archive.org/web/20051004173252/http://www.facebook.com/register.php>] (underlining denotes a hyperlink that was used to link to Facebook’s “Terms of Use”, “Privacy Policy”, etc. webpages).

<sup>78</sup> *Facebook Registration*, Facebook (Mar. 1, 2006), <http://www.facebook.com:80/register.php> [<https://web.archive.org/web/20060301120315/http://www.facebook.com:80/register.php>].

<sup>79</sup> *Register and Start Using Facebook*, Facebook (May 16, 2007), <http://www.facebook.com/r.php> [<https://web.archive.org/web/20070516195245/https://register.facebook.com/r.php>].

<sup>80</sup> *Facebook*, Facebook (May 14, 2008), <http://www.facebook.com> [<https://web.archive.org/web/20080514205157/http://www.facebook.com/>].

<sup>81</sup> *Facebook*, Facebook (Mar. 24, 2009), <http://www.facebook.com> [<https://web.archive.org/web/20090324054710/http://www.facebook.com/>].

**facebook**

Email:  Password:  [Login](#)

☐ Keep me logged in [Forgot your password?](#)

**Facebook helps you connect and share with the people in your life.**

**Sign Up**  
It's free and always will be.

First Name:

Last Name:

Your Email:

Re-enter Email:

New Password:

I am:

Birthday:

[Why do I need to provide this?](#)

[Sign Up](#)

[Create a Page for a celebrity, band or business.](#)

English (US) Español Português (Brasil) Français (France) Deutsch Italiano العربية हिन्दी 中文(简体) 日本語 +

Facebook © 2011 - English (US) [Mobile](#) [Find Friends](#) [Badges](#) [People](#) [Pages](#) [About](#) [Advertising](#) [Developers](#) [Careers](#) [Privacy](#) [Terms](#) [Help](#)

262. Only after users had filled in these six fields of information and affirmatively clicked “Sign Up” were they routed to the following page, which was a pop-up screen that asked users to sign up again after they had already done so, under the guise of a security check:

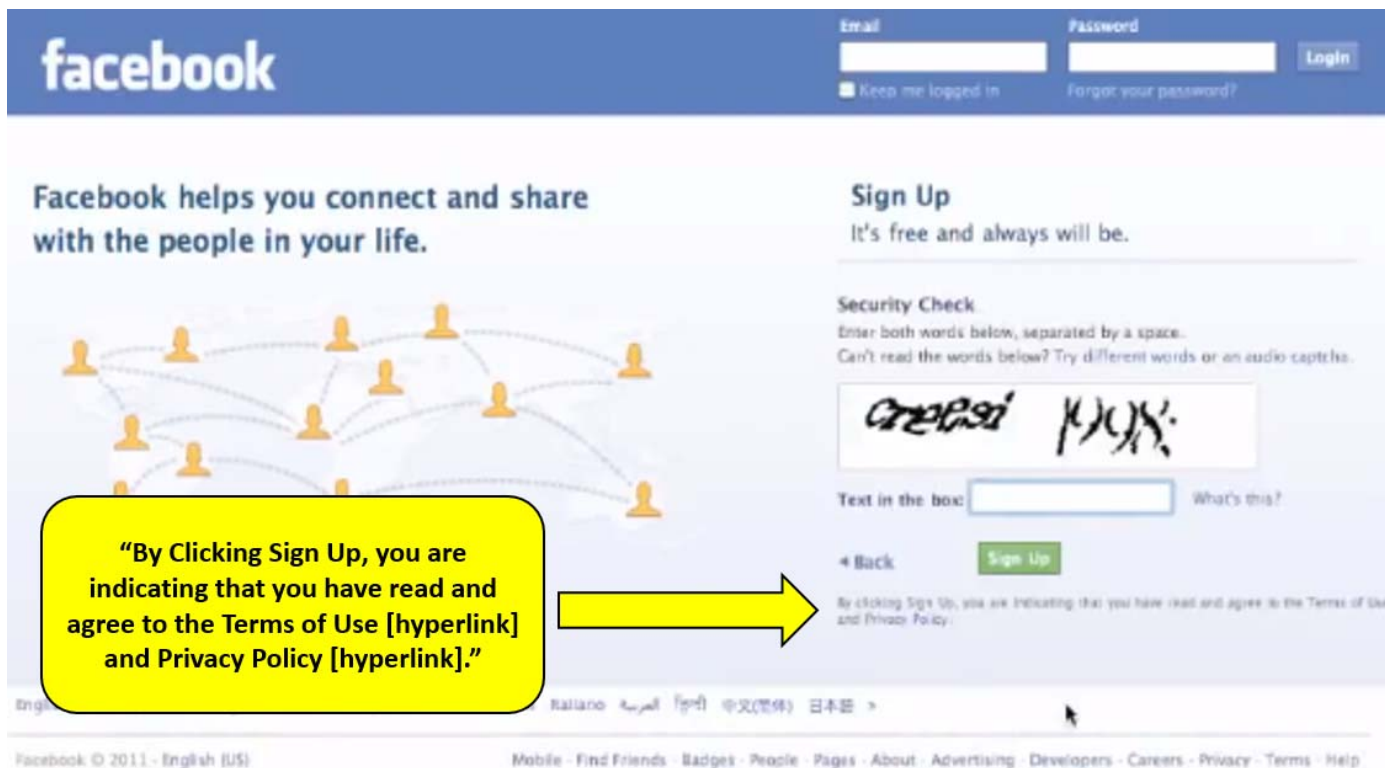


263. This screen required users to engage in a “Security Check.” This check required users to type out the displayed words in a text box. The text on the security screen was distorted such that users would be distracted by and forced to concentrate on the security image.

264. Deceptively, on this same screen and in very small font (likely eight-point in contrast to much larger font above), Facebook placed the following statement below the second sign on screen: “By clicking Sign Up, you are indicating that you have read and agree to the Terms of Use [hyperlink] and Privacy Policy [hyperlink].”<sup>82</sup> Because users had already submitted their own personal information and affirmatively agreed to sign up, they could have easily mistaken or not seen this statement.

<sup>82</sup> *Id.*





265. By 2012, a majority of Americans were on Facebook. As of December 31, 2011, Facebook had 161 million monthly active users (“MAUs”) in the United States.<sup>83</sup> Facebook narrowly defined a MAU as “as a registered Facebook user who logged in and visited Facebook through our website or a mobile device, or took an action to share content or activity with his or her Facebook friends or connections via a third-party website that is integrated with Facebook, in the last 30 days as of the date of measurement. MAUs are a measure of the size of our global active user community, which has grown substantially in the past several years.” The \$161 million figure therefore underestimates the number of registered Facebook users at that time. Moreover, as of December 31, 2012, “more than 10 million apps and websites were integrated

<sup>83</sup> Facebook, Inc., Amendment No. 2 to Form S-1 (Form S-1/A) (Mar. 7, 2012), <https://www.sec.gov/Archives/edgar/data/1326801/000119312512101422/d287954ds1a.htm>; see also United States Census Bureau (Dec. 29, 2011), <https://www.census.gov/newsroom/releases/archives/population/cb11-219.html> (The U.S. population was 312.8 million at that time.).

with Facebook.”<sup>84</sup> Accordingly, at least 161 million Facebook users in the United States had signed up with Facebook in one of the ways just described. Millions more U.K. users also signed up.

266. In February 2012, Facebook changed its sign-up page again to include the following statement: “By clicking Sign Up, you agree to our Terms [hyperlinked] and that you have read and understand our Data Use Policy [hyperlinked].”<sup>85</sup> As discussed in more detail below, at this point Facebook had changed its “Privacy Policy” to a “Data Use Policy,” making it less likely that a consumer concerned about privacy would read it. An example from 2012 is shown below:<sup>86</sup>

<sup>84</sup> Facebook, Inc., Annual Report (Form 10-k) at 6 (Dec. 31, 2012), <https://www.sec.gov/Archives/edgar/data/1326801/000132680113000003/fb-12312012x10k.htm>.

<sup>85</sup> *Your Facebook Timeline*, Facebook (Feb. 9, 2012), <http://www.facebook.com> [<https://web.archive.org/web/20120209101026/http://www.facebook.com/>].

<sup>86</sup> *Id.*



267. In May 2012, this statement changed again to state: “By clicking Sign Up, you agree to our Terms [hyperlinked] and that you have read our Data Use Policy [hyperlinked], including our Cookie Use [hyperlinked].”<sup>87</sup> Notably, this statement does not require agreement to its Data Use Policy. Rather, it provides only a statement that the user has read the Policy.

268. Beginning in January 2017, this statement changed to include the following language: “By clicking Create Account, you agree to our Terms [hyperlinked] and that you have read our Data Policy [hyperlinked], including our Cookie Use [hyperlinked]. You may receive SMS Notifications from Facebook and can opt out at any time.”<sup>88</sup>

269. Finally, as of April 2018, Facebook changed this statement to read: “By clicking Sign Up, you agree to our Terms [hyperlinked], Data Policy [hyperlinked] and Cookies Policy [hyperlinked]. You may receive SMS Notifications from us and can opt out any time.”<sup>89</sup>

270. Facebook signed up new users at a significantly lower rate after 2012. Statista, an online statistics, market research, and business intelligence service, estimates that in 2015, there were 192 million Facebook users in the United States and as of 2018, that number had grown to 207 million.<sup>90</sup> Thus, from December 31, 2011 to January 2018, the number of Facebook users in the United States grew less than 50 million.

**c. The Privacy, Data Use, and Data Policies Made It Difficult for Users to Understand How Facebook Made Their Content and Information Accessible to Third Parties**

271. Facebook made it difficult for its users to understand that third parties were constantly vacuuming up their content and information and that Facebook was not monitoring

---

<sup>87</sup> *Sign Up*, Facebook (May 27, 2012), <http://www.facebook.com> [<https://web.archive.org/web/20120527094845/http://www.facebook.com/>].

<sup>88</sup> *Sign Up*, Facebook (Jan. 2, 2017), <https://www.facebook.com> [<https://web.archive.org/web/20170102180912/https://www.facebook.com/>].

<sup>89</sup> *Sign Up*, Facebook (Apr. 20, 2018), <https://www.facebook.com> [<https://web.archive.org/web/20180420095336/https://www.facebook.com/>].

<sup>90</sup> *Number of Facebook Users in the United States from 2015-2022*, Statista (2018), <https://www.statista.com/statistics/408971/number-of-us-facebook-users/>.

what they did with it.

272. Although the Statement of Rights and Responsibilities contained a link to a “Platform Page” so that users could “learn more about Platform,” there was no other information that indicated what “Platform” was or why users would want or need to read that page.

273. The Data Use Policy that was dated December 9, 2009 and went unchanged until April 22, 2010 did not adequately disclose what information third parties could access from friends. In fact, the relevant section in this policy is labeled, “Information You Share With Third Parties.” This section falsely states:

We take steps to ensure that others use information that you share on Facebook in a manner consistent with your privacy settings [hyperlinked], but we cannot guarantee that they will follow our rule.

You can use your application settings [hyperlink] to limit which of your information your friends can make available to applications and websites.<sup>91</sup>

However, this section provides no further detail about the level of information available on Graph API v1.0. Experts have rightly criticized this as a hidden back door, overriding the privacy choices users made by users about what content they are actually sharing.

274. The April 22, 2010 version of the Data Use Policy includes the following language:

**When your friends use Platform.** If your friend connects with an application or website, it will be able to access your name, profile picture, gender, user ID, and information you have shared with “everyone.” It will also be able to access your connections, except it will not be able to access your friend list. If you have already connected with (or have a separate account with) that website or application, it may also be able to connect you with your friend on that application or website. If the application or website wants to access any of your other content or information (including your friend list), it will have to obtain specific permission from your friend. If your friend grants specific permission to the application or website, it will generally only be able to access content and information about you that your friend can access. In addition, it will only be allowed to use that content and information in connection with that friend. For example, if a friend gives an application access to a photo you only shared with your friends, that application could allow your friend to view or print the photo, but it cannot show that photo to anyone else.

---

<sup>91</sup> *Facebook’s Privacy Policy*, Facebook (Apr. 2, 2010), <http://www.facebook.com/policy.php> [<https://web.archive.org/web/20100402021414/facebook.com/policy.php>].

...

We provide you with a number of tools to control how your information is shared when your friend connects with an application or website. For example, you can use your Application and Websites privacy setting [hyperlink] to limit some of the information your friends can make available to applications and websites. You can block all platform applications and websites completely or block particular applications or websites from accessing your information. You can use your privacy settings to limit which friends can access your information, or limit which of your information is available to “everyone.” You can use your privacy settings [hyperlinked] to limit which friends can access your information, or limit which of your information is available to “everyone.”<sup>92</sup>

275. On September 7, 2011, Facebook changed the Data Policy so that it contained a section titled, “Controlling what is shared when the people you share with use applications.”<sup>93</sup>

This section states:

Just like when you share information by email or elsewhere on the web, information you share on Facebook can be re-shared. This means that if you share something on Facebook, anyone who can see it can share it with others, including the games, applications, and websites they use.

Your friends and the other people you share information with often want to share your information with applications to make their experiences on those application more personalized and social. For example, one of your friends might want to use a music application that allows them to see what their friends are listening to. To get the full benefit of that application, your friend would want to give the application her friend list – which includes your User ID - so the application knows which of her friends is also using it. Your friend might also want to share the music you "like" on Facebook. If you have made that information public, then the application can access it just like anyone else. But if you’ve shared your likes with just your friends, the application could ask your friend for permission to share them.

You can control most of the information other people share with applications using you Apps and Websites [hyperlinked] settings. But these controls do not let you limit access to your public information and friend list.

---

<sup>92</sup> *Data Use Policy*, Facebook (Sept. 22, 2011), <http://www.facebook.com/about/privacy/your-info-on-other> [https://web.archive.org/web/20110922202503/http://www.facebook.com/about/privacy/your-info-on-other].

<sup>93</sup> *Data Use Policy*, Facebook (Sept. 7, 2011), <http://www.facebook.com/about/privacy/your-info-on-other> [https://web.archive.org/web/20110922202503/http://www.facebook.com/about/privacy/your-info-on-other].

If you want to completely block applications from getting your information, you will need to turn off all Platform applications [hyperlinked]. This means that you will no longer be able to use any games, applications or websites.

If an application asks permission from someone else to access your information, the application will be allowed to use that information only in connection with the person that gave the permission and no one else.<sup>94</sup>

276. This language did not change in any meaningful way until the January 30, 2015 Data Policy,<sup>95</sup> which states, under the section “Sharing On Our Services”:

Information from third-party partners.

We receive information about you and your activities on and off Facebook from third-party partners, such as information from a partner when we jointly offer services or from an advertiser about your experiences or interactions with them.

...

People you share and communicate with.

When you share and communicate using our Services, you choose the audience who can see what you share. For example, when you post on Facebook, you select the audience for the post, such as a customized group of individuals, all of your Friends, or members of a Group. Likewise, when you use Messenger, you also choose the people you send photos to or message.

Public information is any information you share with a public audience, as well as information in your Public Profile, or content you share on a Facebook Page or another public forum. Public information is available to anyone on or off our Services and can be seen or accessed through online search engines, APIs, and offline media, such as on TV.

In some cases, people you share and communicate with may download or re-share this content with others on and off our Services. When you comment on another person’s post or like their content on Facebook, that person decides the audience who can see your comment or like. If their audience is public, your comment will also be public.

---

<sup>94</sup> *Privacy Policy*, Facebook (Sept. 23, 2011), [http://www.facebook.com/full\\_data\\_use\\_policy](http://www.facebook.com/full_data_use_policy) [[https://web.archive.org/web/20111013084008/http://www.facebook.com/full\\_data\\_use\\_policy](https://web.archive.org/web/20111013084008/http://www.facebook.com/full_data_use_policy)].

<sup>95</sup> The following sentence was added to the end of this section in the November 15, 2013 Data Policy: “For example, some apps use information such as your friends list, to personalize your experience or show you which of your friends use that particular app.” *Data Use Policy - Other Websites and Applications*, Facebook (Nov. 4, 2014), <https://www.facebook.com/about/privacy/your-info-on-other> [<https://web.archive.org/web/20141104152550/https://www.facebook.com/about/privacy/your-info-on-other>].

People that see content others share about you.

Other people may use our Services to share content about you with the audience they choose. For example, people may share a photo of you, mention or tag you at a location in a post, or share information about you that you shared with them. If you have concerns with someone's post, social reporting is a way for people to quickly and easily ask for help from someone they trust. [Learn More](#) [hyperlink].

Apps, websites and third-Party integrations on or using our Services.

When you use third-party apps, websites or other services that use, or are integrated with, our Services, they may receive information about what you post or share. For example, when you play a game with your Facebook friends or use the Facebook Comment or Share button on a website, the game developer or website may get information about your activities in the game or receive a comment or link that you share from their website on Facebook. In addition, when you download or use such third-party services, they can access your [Public Profile](#) [hyperlink], which includes your [username or user ID](#) [hyperlink], your age range and country/language, your list of friends, as well as any information that you share with them. Information collected by these apps, websites or integrated services is subject to their own terms and policies.

[Learn more](#) [hyperlink] about how you can control the information about you that you or others share with these apps and websites.

277. Facebook's Data policies also contain the following language regarding service providers, but that language was vague and did not clearly disclose that when a users' friends accessed Facebook through these service providers, all of a user's content and information would be available to that service provider without restriction. For example, in the May 24, 2007 Policy, Facebook stated:<sup>96</sup>

We may provide information to service providers to help us bring you the services we offer. Specifically, we may use third parties to facilitate our business, such as to host the service at a co-location facility for servers, to send out email updates about Facebook, to remove repetitive information from our user lists, to process payments for products or services, to offer an online job application process, or to provide search results or links (including sponsored links). In connection with these offerings and business operations, our service providers may have access to your personal information for use for a limited time in connection with these business activities. Where we utilize third parties for the processing of any personal information, we implement reasonable contractual and technical

---

<sup>96</sup> *Facebook: Facebook's Privacy Policy* (June 30, 2007), <https://www.facebook.com/policy.php> [<https://web.archive.org/web/20070630042429/facebook.com/policy.php>].

protections limiting the use of that information to the Facebook-specified purposes.

...

We may offer stores or provide services jointly with other companies on Facebook. You can tell when another company is involved in any store or service provided on Facebook, and we may share customer information with that company in connection with your use of that store or service

278. This disclosure stated only that access was “utilized” for a period of time. It did not mention software makers, mobile carriers, etc.

279. This language was changed in the December 9, 2009 Privacy Policy to the following:<sup>97</sup>

**To provide you with services.** We may provide information to service providers that help us bring you the services we offer. For example, we may use third parties to help host our website, send out email updates about Facebook, remove repetitive information from our user lists, process payments, or provide search results or links (including sponsored links). These service providers may have access to your personal information for use for a limited time, but when this occurs we implement reasonable contractual and technical protections to limit their use of that information to helping us provide the service.

280. This disclosure also failed to clearly state that users’ content and information was fully available to services providers. And like the other disclosures set forth herein, it does not set forth controls Facebook had in place to protect user data.

281. Facebook continued to unilaterally change the terms of the Data Policy, but did not give meaningful notice for any of them. In 2011, Facebook changed its language to the following:<sup>98</sup>

### **Service Providers**

---

<sup>97</sup> *Facebook: Facebook’s Privacy Policy*, Facebook § 4 (Apr. 2, 2010), <https://www.facebook.com/policy.php> [<https://web.archive.org/web/20100402021414/facebook.com/policy.php>].

<sup>98</sup> *Facebook: Data Use Policy*, Facebook § 4 (Jan. 12, 2012), <http://www.facebook.com/about/privacy/> [<https://web.archive.org/web/20120112083418/http://www.facebook.com/about/privacy/>].

We give your information to the people and companies that help us provide the services we offer. For example, we may use outside vendors to help host our website, serve photos and videos, process payments, or provide search results. In some cases we provide the service jointly with another company, such as the Facebook Marketplace. In all of these cases our partners must agree to only use your information consistent with the agreement we enter into with them, as well as this privacy policy.

282. On June 8, 2012, this language changed to read:<sup>99</sup>

**Service Providers**

We give your information to the people and companies that help us provide, understand and improve the services we offer. For example, we may use outside vendors to help host our website, serve photos and videos, process payments, analyze data, measure the effectiveness of ads, or provide search results. In some cases we provide the service jointly with another company, such as the Facebook Marketplace. In all of these cases our partners must agree to only use your information consistent with the agreement we enter into with them, as well as this Data Use Policy.

283. On December 11, 2012 this language altered slightly to include the following:<sup>100</sup>

**Service Providers**

We give your information to the people and companies that help us provide, understand and improve the services we offer. For example, we may use outside vendors to help host our website, serve photos and videos, process payments, analyze data, **conduct and publish research**, measure the effectiveness of ads, or provide search results. In some cases we provide the service jointly with another company, such as the Facebook Marketplace. In all of these cases our partners must agree to only use your information consistent with the agreement we enter into with them, as well as this Data Use Policy.

284. The language changed again on January 30, 2015 to read:<sup>101</sup>

---

<sup>99</sup> *Facebook: Data Use Policy*, Facebook § 6 (June 24, 2012), <http://www.facebook.com/about/privacy/> [[https://web.archive.org/web/20120624132517/http://www.facebook.com/full\\_data\\_use\\_policy](https://web.archive.org/web/20120624132517/http://www.facebook.com/full_data_use_policy)].

<sup>100</sup> *Facebook: Data Use Policy*, Facebook § 6 (Apr. 15, 2013), <http://www.facebook.com/about/privacy/> [[https://web.archive.org/web/20130415134127/https://www.facebook.com/full\\_data\\_use\\_policy](https://web.archive.org/web/20130415134127/https://www.facebook.com/full_data_use_policy)].

<sup>101</sup> *Facebook: Data Use Policy*, Facebook § 3 (Aug. 17, 2016), <http://www.facebook.com/about/privacy/> [<https://web.archive.org/web/20150817185318/facebook.com/policy.php>].



**Vendors, service providers and other partners.** We transfer information to vendors, service providers, and other partners who globally support our business, such as providing technical infrastructure services, analyzing how our Services are used, measuring the effectiveness of ads and services, providing customer service, facilitating payments, or conducting academic research and surveys. These partners must adhere to strict confidentiality obligations in a way that is consistent with this Data Policy and the agreements we enter into with them

This language did not change until April 2018.

285. As with the third-party application disclosures, the many pages and paragraphs were intended to obscure what was really happening with users' content and information. It is only following a Congressional investigation that Facebook admitted that it believes its "partners" have the same authority as Facebook to access and curate data. None of these disclosures say so.

**d. The Documents Were Constantly Changing**

286. Facebook has repeatedly changed the names of its documents. For example, prior to 2009, Facebook referred to its main "Terms" policy as the "Terms of Use." Beginning with the policy published on May 1, 2009, Facebook changed this name to the "Statement of Rights and Responsibilities." Likewise, Facebook's changed the name of its policy that was available to users when they click on the hyperlink "privacy" at the bottom of the Facebook landing page. This policy was originally labelled "Privacy Policy." Facebook then changed that name to the "Data Use Policy" in September 2012, and again changed the name to the "Data Policy" in January 2015.

287. From October 2005 to August 2018, Facebook published twenty different "Terms of Use" and Statements of Rights and Responsibilities. During that same time frame, Facebook published 20 distinct Privacy Policies, Data Use Policies, and Data Policies. Upon information and belief, Facebook failed to notify Plaintiffs and Class Members of these changes.

288. From April 2010 (the time the Platform Policies were created) to August 2018, Facebook published 40 different Platform Policies. In total, a user who signed up in 2005 would have had to read 80 different policies in order to know what information third parties had access to. Even from just the period of April 2010 to May 2015 (the period where Graph API v1.0 was



operational), a user would have been responsible for 8 Statements of Rights and Responsibilities, 9 Data Use Policies and 28 Platform Policies—45 total policies. A chart listing these publishing dates is shown below:

	<b>Terms of Use and Statement of Rights and Responsibilities –Publishing Dates (20 Total)</b>	<b>Privacy, Data Use, and Data Policy –Publishing Dates (20 Total)</b>	<b>Platform Policy –Publishing Dates (40 Total)</b>
1.		06/28/2005	
2.	10/03/2005		
3.	02/27/2006	02/27/2006	
4.		05/22/2006	
5.		09/05/2006	
6.	10/23/2006	10/23/2006	
7.	12/13/2006		
8.	05/24/2007	05/24/2007	
9.	11/15/2007		
10.	6/07/2008		
11.	09/23/2008		
12.		11/26/2008	
13.	05/01/2009 –Name changed to “Statement of Rights and Responsibilities”		
14.	08/28/2009		
15.		12/09/2009	
16.	12/21/2009		
17.			04/21/2010
18.	04/22/2010	04/22/2010	
19.			06/29/2010
20.			07/27/2010
21.	08/25/2010		
22.	10/04/2010		
23.		10/05/2010	
24.			10/22/2010
25.			10/29/2010
26.			11/15/2010
27.		12/22/2010	12/22/2010
28.			02/10/2011
29.	04/26/2011		
30.			05/24/2011
31.			07/01/2011
32.			07/27/2011
33.			08/12/2011

	<b>Terms of Use and Statement of Rights and Responsibilities –Publishing Dates (20 Total)</b>	<b>Privacy, Data Use, and Data Policy –Publishing Dates (20 Total)</b>	<b>Platform Policy –Publishing Dates (40 Total)</b>
34.		09/07/2011 –Name changed to “Data Use Policy”	
35.			09/22/2011
36.		09/23/2011	
37.			10/10/2011
38.			12/15/2011
39.			03/06/2012
40.			04/25/2012
41.	06/08/2012	06/08/2012	
42.			09/12/2012
43.	12/11/2012	12/11/2012	
44.			12/12/2012
45.			01/25/2013
46.			02/20/2013
47.			04/09/2013
48.			06/28/2013
49.			08/20/2013
50.	11/15/2013	11/15/2013	
51.			May 2014*
52.			September 2014*
53.			11/05/2014
54.	01/30/2015	1/30/2015 –Name changed to “Data Policy”	
55.			03/25/2015
56.			04/12/2016
57.			05/26/2016
58.			08/30/2016
59.		09/29/2016	
60.			03/13/2017
70.			04/18/2017
71.			05/15/2017
72.			08/29/2017
73.			10/27/2017
74.			03/14/2018
75.			04/24/2018
76.	04/19/2018	04/19/2018	
77.			05/07/2018

\*From May 2014 to November 2014, Facebook omitted any associated publication date for its Platform Policies. Based upon counsel's investigation, Facebook issued at least two materially different policies.<sup>102</sup> Without a publication date, no user could have reasonably understood when these policies had changed.

289. This constant stream of policies worked to effectively drown users in information and hide the fact that third parties could access users' content and information. Providing notice of policy updates is important because most Facebook users do not read the terms of service.<sup>103</sup>

290. Indeed, Facebook intended that users would never read the Statement of Rights and Responsibilities or its data policies. Facebook's policies are posted separately from users' interactions with its platform. Only the persistently curious user could find the relevant policies on Facebook's website, which are buried in obscure corners of the website and take dozens of clicks to find. "So how many clicks does it take to protect ... your privacy from third-party apps? About two dozen, assuming my fictional Facebook self is a competent novice."<sup>104</sup>

**e. Facebook Failed to Adequately Notify Users of Changes to the Privacy Policy, Data Policy, and Data Use Policy**

291. Even though Facebook's Privacy Policy (and later Data Policy and Data Use Policy) continued to change throughout the Class Period, Facebook failed to adequately notify its users when it updated it. From December 2012 to January 2015, Facebook's method of notification was "by publication [on the Data Use Policy webpage] and on the Facebook Site

---

<sup>102</sup> See *Platform Policy*, Facebook (May 12, 2014), <https://developers.facebook.com/policy> [<https://web.archive.org/web/20140512215731/developers.facebook.com/policy>]; see also *Platform Policy*, Facebook (Sept. 12, 2014), <https://developers.facebook.com/policy> [<https://web.archive.org/web/20140912214833/https://developers.facebook.com/policy/>].

<sup>103</sup> Kimberlee Morrison, *Survey: Many Users Never Read Social Networking Terms of Service Agreements*, Adweek (May 27, 2015), <https://www.adweek.com/digital/survey-many-users-never-read-social-networking-terms-of-service-agreements/>.

<sup>104</sup> Laura Hautala, *Facebook Privacy Settings Make You Work to Stop the Data Sharing*, CNET (Mar. 22, 2018), <https://www.cnet.com/news/how-to-stop-sharing-facebook-data-after-cambridge-analytica-mess/>.

Governance Page.”<sup>105</sup> In other words, Facebook would *not* notify users of changes to the Data Use Policy unless a user happened to be in the habit of checking the Data Use Policy webpage or the Facebook Site Governance Page on a daily basis.

292. After January 2015, Facebook’s vow was even vaguer; it simply said, “We’ll notify you before we make changes to this policy and give you the opportunity to review and comment on the revised policy before continuing to use our Services.”<sup>106</sup> Facebook did not specify how it would notify users, where it would post the draft revised policy for review and comment, or how users would comment on the draft or decline to consent to a new policy.

293. As a result, users were not notified of and did not consent to revisions of the Data Policy after the users initially joined Facebook.

**E. The Cambridge Analytica Scandal and Subsequent Revelations of Facebook’s Agreements with Third Parties to Share User Content and Information with Third Parties Without Full Disclosure Show that Facebook Violated the 2012 Federal Trade Commission Consent Decree**

294. In 2009, the nonprofit organization Electronic Privacy Information Center (“EPIC”), a public interest research center in Washington, D.C., filed a complaint and request for investigation, injunction, and other relief against Facebook before the Federal Trade Commission (“FTC”).<sup>107</sup>

295. EPIC’s complaint alleged that the Facebook Platform transferred Facebook users’ personal data to application developers without users’ knowledge or consent. Specifically, the complaint stated:

55. Facebook permits third-party applications to access user information at the moment a user visits an application website. According to Facebook, third party applications

---

<sup>105</sup> *Data Use Policy*, Facebook (Dec. 11, 2012), [https://www.facebook.com/full\\_data\\_use\\_policy](https://www.facebook.com/full_data_use_policy) [[https://web.archive.org/web/20130415134127/https://www.facebook.com/full\\_data\\_use\\_policy](https://web.archive.org/web/20130415134127/https://www.facebook.com/full_data_use_policy)].

<sup>106</sup> *Data Use Policy*, Facebook (Sept. 29, 2016), <https://www.facebook.com/policy.php> [<https://web.archive.org/web/20180414092121/https://www.facebook.com/policy.php>].

<sup>107</sup> EPIC Complaint, Request for Investigation, Injunction, and Other Relief, *In re Facebook, Inc.* (F.T.C. Dec. 17, 2009), <https://www.epic.org/privacy/inrefacebook/EPIC-FacebookComplaint.pdf>

receive publicly available information automatically when you visit them, and additional information when you formally authorize or connect your Facebook account with them.

56. As Facebook itself explains in its documentation, when a user adds an application, by default that application then gains access to everything on Facebook that the user can see. The primary “privacy setting” that Facebook demonstrates to third-party developers governs what other users can see from the application’s output, rather than what data may be accessed by the application.

...

64. With the Preferred Developer Program, Facebook will give third-party developers access to a user’s primary email address, personal information provided by the user to Facebook to subscribe to the Facebook service, but not necessarily available to the public or to developers. In fact, some users may choose to create a Facebook account precisely to prevent the disclosure of their primary email address.

...

68. Under the revised settings, even when a user unchecks all boxes and indicates that none of the personal information listed above should be disclosed to third party application developers, Facebook states that “applications will always be able to access your publicly available information (Name, Profile Picture, Gender, Current City, Networks, Friend List, and Pages) and information that is visible to Everyone.”

...

70. Facebook does not now provide the option that explicitly allows users to opt out of disclosing all information to third parties through the Facebook Platform.

71. Users can block individual third-party applications from obtaining personal information by searching the Application Directory, visiting the application’s “about” page, clicking a small link on that page, and then confirming their decision. A user would have to perform these steps for each of more than 350,000 applications in order to block all of them.<sup>108</sup>

296. The FTC investigated EPIC’s claims. On November 29, 2011, the FTC announced that Facebook had agreed to settle FTC charges that Facebook had “deceived consumers by telling them they could keep their information on Facebook private, and then repeatedly allowing it to be shared and made public.” The FTC released a proposed consent decree for public comment.

297. On July 27, 2012, the FTC finalized and issued its Consent Decree, which

---

<sup>108</sup> *Id.*

ordered, in part, that Facebook:

[S]hall not misrepresent in any manner, expressly or by implication, the extent to which it maintains the privacy or security of covered information, including, but not limited to:

- A. its collection or disclosure of any covered information;
- B. the extent to which a consumer can control the privacy of any covered information maintained by [Facebook] and the steps a consumer must take to implement such controls;
- C. the extent to which [Facebook] makes or has made covered information accessible to third parties;
- D. the steps [Facebook] takes or has taken to verify the privacy or security protections that any third party provides . . . .<sup>109</sup>

298. The Consent Decree further ordered, in part, that Facebook:

[p]rior to any sharing of a user's nonpublic user information by [Facebook] with any third party, which materially exceeds the restrictions imposed by a user's privacy setting(s), shall:

- A. clearly and prominently disclose to the user, separate and apart from any "privacy policy," "data use policy," "statement of rights and responsibilities" page, or other similar document: (1) the categories of nonpublic user information that will be disclosed to such third parties, (2) the identity or specific categories of such third parties, and (3) that such sharing exceeds the restrictions imposed by the privacy setting(s) in effect for the user; and
- B. obtain the user's affirmative express consent.<sup>110</sup>

299. Facebook violated the Consent Decree in several different ways. *First*, it failed to "clearly and prominently disclose" how users' information could be shared with third-party apps via their friends. *Second*, it failed to make that disclosure "separate and apart from" its Privacy Policy, Data Use Policy, and Statement of Rights and Responsibilities. *Third*, far from obtaining users' affirmative express consent, Facebook's default setting was that users' personal information could be shared with third-party apps via the users' friends. *Fourth*, by putting a user's application-related privacy settings on a page completely different from all other privacy

---

<sup>109</sup> Decision and Order ("Consent Decree"), *In the Matter of Facebook, Inc.*, at 3-4, No. C-4365 (F.T.C. July 27, 2012).

<sup>110</sup> *Id.* at 4.

settings, Facebook misrepresented, by implication, the extent to which it maintained the privacy or security of users' content and information.

300. By sharing its users' data with third parties, as described in detail above, Facebook has violated the terms of the FTC's July 27, 2012 Consent Decree.

**F. Even Prior to the Cambridge Analytica Scandal, Numerous Investigations Questioned Facebook's Practices With Regard to User Privacy**

301. In 2012, Facebook faced a class action lawsuit from users for sharing users' "likes" of advertisers without compensation or allowing them to opt out. Facebook settled this case for \$20 million.

302. On May 14, 2015, a class action lawsuit was filed against Facebook alleging that Facebook's photo scanning technology violates users' privacy rights.

303. In June 2015, The Belgium Privacy Commission filed a lawsuit against Facebook over alleging that Facebook broke the privacy law of Belgium and the European Union laws by tracking people on third-party sites without first obtaining their consent. In February 2018, a Belgian court ordered Facebook to stop this practice or face daily fines.<sup>111</sup>

304. In 2016, Germany's Consumer Federation announced it would fine Facebook €100,000 for failing to comply with a previous court order requiring Facebook to make clear the extent to which users' intellectual property "could be used by Facebook and licensed to third parties."

305. In March 2017, the ICO, an independent body set up to uphold information rights, began looking into whether personal data acquired from Facebook had been misused by campaigns. On July 10, 2018, the ICO announced it would fine FB 500,000 euros, the maximum allowable under the law, for two breaches of Britain's 1998 Data Protection Act. "The ICO's investigation concluded that Facebook contravened the law by failing to safeguard people's information. It also found that the company failed to be transparent about how people's data was

---

<sup>111</sup> Samuel Gibbs, *Facebook Ordered to Stop Collecting User Data by Belgian Court*, Guardian (Feb. 16, 2018), <https://www.theguardian.com/technology/2018/feb/16/facebook-ordered-stop-collecting-user-data-fines-belgian-court>.

harvested by others.”<sup>112</sup>

306. On May 16, 2017, the Dutch and French Data Protection Authorities (“DPA”) announced that Facebook had not provided users sufficient control over how their information was being used. The French DPA fined Facebook €150,000 for failure to stop tracking non-users’ web activity without their consent and transferring personal information to United States.<sup>113</sup> The French DPA stated: “the cookie banner and the mention of information collected ‘on and outside Facebook’ do not allow users to clearly understand that their personal data are systematically collected as soon as they navigate on a third-party website that includes a social plug in.”<sup>114</sup>

307. On May 18, 2017, the European Union’s antitrust commission fined Facebook \$122 million for misleading regulators about combining data from the messaging service app WhatsApp.

308. In September 2017, the Spanish data protection authority (the AEPD) fined Facebook €1.2 million (\$1.44 million) for its collection of data on “people’s ideologies and religious beliefs, sex and personal tastes” without users consent and for not deleting information that was not relevant.

**G. Despite Warnings, Facebook Failed to Take Reasonable Measures to Ensure That Third-Party Applications and Device Makers Would Not Access and Use Its Users’ Content and Information Without Their Consent.**

309. Third parties’ unauthorized access to and use of Plaintiffs’ content and information should not—indeed did not—come as a surprise to Facebook when it was revealed to the public in 2018. Facebook had disregarded earlier red flags and had failed to implement reasonable measures to secure its users’ data.

---

<sup>112</sup> *Findings, Recommendations and Actions From ICO Investigation Into Data Analytics in Political Campaigns*, ICO (July 10, 2018), <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/07/findings-recommendations-and-actions-from-ico-investigation-into-data-analytics-in-political-campaigns/>.

<sup>113</sup> *Common Statement by the Contact Group of the Data Protection Authorities of the Netherlands, France, Spain, Hamburg and Belgium*, CNIL (May 16, 2017), <https://www.cnil.fr/fr/node/23602>.

<sup>114</sup> *Id.*



**1. Facebook Partnered With Kogan to Exploit Facebook User Data for Commercial Use**

310. Facebook was well aware of the commercial use of personal content and information through the MyDigitalLife app. GSR's "End User Terms and Conditions" were posted publicly. Kogan has stated that he "never heard a word" from Facebook concerning his intent to "sell" data even though he had publicly posted his intention for a year and a half.

311. Facebook became aware that Kogan and GSR had misused data after the *Guardian* published an article about it in December 11, 2015. Facebook then conducted an investigation.

312. At minimum, Facebook became aware that GSR had sold Facebook data containing personal content by March 2016, in negotiating with Kogan a settlement of claims, when Facebook was informed that Kogan generated revenues by re-selling Facebook user data. Facebook failed to determine at that time the scope and extent of the content and information GSR had obtained. Indeed, Facebook waited over two years to make any type of public disclosure.

**2. Facebook Has Repeatedly Ignored Its Users' Privacy Rights and Expectations**

313. Throughout its history, Facebook has continually pushed past users' privacy concerns seeking to maximize its growth and maximize its profits. In light of the company's history of privacy abuses, it is apparent that the company's motto to "move fast and break things" applies even to users' privacy.

314. In 2006, Facebook unveiled its News Feed feature. This feature soon faced controversy since users' posts were automatically revealed regardless of users' intention to keep these posts private. Zuckerberg's response to this controversy was that "we did a bad job of explaining what the new features were and an even worse job of giving you control of them."<sup>115</sup>

315. In 2007, Facebook launched Beacon. This feature automatically enrolled users into sharing their website and app history with advertisers. Users were sometimes unaware of

---

<sup>115</sup> Mark Zuckerberg, *An Open Letter From Mark Zuckerberg*, Facebook (Sept. 8, 2006), <https://www.facebook.com/notes/facebook/an-open-letter-from-mark-zuckerberg/2208562130/>.

these posts, and the sites also gave Facebook ad-targeting data. After privacy complaints and a class action lawsuit, Beacon was shut down. In response, Zuckerberg stated, “We’ve made a lot of mistakes building this feature, but we’ve made even more with how we’ve handled them. We simply did a bad job with this release, and I apologize for it.”<sup>116</sup>

316. In 2009, the Facebook faced a complaint by the Canadian Internet Policy and Public Interest Clinic (“CIPPIC”) over a number of privacy concerns including the information shared by users to third party app developers. This complaint resulted in an investigation by the Canadian Privacy Commissioner (“CPC”). As a result of this investigation, the CPC announces the following:

Facebook has agreed to retrofit its application platform in a way that will prevent any application from accessing information until it obtains express consent for each category of personal information it wishes to access. Under this new permissions model, users adding an application will be advised that the application wants access to specific categories of information. The user will be able to control which categories of information an application is permitted to access. There will also be a link to a statement by the developer to explain how it will use the data.<sup>117</sup>

317. Yet this settlement did not stop Facebook from continuing to exploit users’ privacy. In May 2010, the *Wall Street Journal* reported that Facebook had been sending users’ names and Facebook Identification numbers to advertising companies. This information was being sent without users’ consent. In his apology, Zuckerberg stated, “Sometimes we move too fast—and after listening to recent concerns, we’re responding.”<sup>118</sup>

318. In July 2010, while giving a speech at a technology awards show in San Francisco, Zuckerberg announced that privacy is no longer a “social norm.”<sup>119</sup> Zuckerberg

---

<sup>116</sup> Mark Zuckerberg, *Thoughts on Beacon*, Facebook (Dec. 5, 2007), <https://www.facebook.com/notes/facebook/thoughts-on-beacon/7584397130/>.

<sup>117</sup> Office of the Privacy Commissioner of Canada, *Facebook Agrees to Address Privacy Commissioner’s Concerns*, OPC (Aug. 27, 2009), [https://www.priv.gc.ca/en/opc-news/news-and-announcements/2009/nr-c\\_090827/](https://www.priv.gc.ca/en/opc-news/news-and-announcements/2009/nr-c_090827/).

<sup>118</sup> Mark Zuckerberg, *From Facebook, Answering Privacy Concerns with New Settings*, Wash. Post (May 24, 2010), <http://www.washingtonpost.com/wp-dyn/content/article/2010/05/23/AR2010052303828.html>.

<sup>119</sup> Bobbie Johnson, *Privacy No Longer a Social Norm, Says Facebook Founder*, Guardian (Jan. 10, 2010), <https://www.theguardian.com/technology/2010/jan/11/facebook-privacy>.

stated, “People have really gotten comfortable not only sharing more information and different kinds, but more openly and with more people. That social norm is just something that has evolved over time.”<sup>120</sup> Zuckerberg’s proclamation that social norms have changed serves as a thin veil to Facebook’s continued violation of users’ privacy.

319. Statements from other executives at Facebook show the same reckless determination to grow. For example, in 2016, Andrew Bosworth, a vice president at Facebook, defended the company’s growth tactics in an internal memo. Bosworth’s memo explains that despite any ramifications, Facebook’s growth is “\*de facto\* good”:

The ugly truth is that we believe in connecting people so deeply that anything that allows us to connect more people more often is \*de facto\* good. It’s perhaps the only area where the metrics do tell the true story as far as we are concerned.

...

[M]ake no mistake, growth tactics are how we got here. If you joined the company because it is doing great work, that’s why we get to do that great work. We do have great products but we still wouldn’t be half our size without pushing the envelope on growth. Nothing makes Facebook as valuable as having your friend on it, and no product decisions have gotten as many friends on as the ones made in growth.

320. The reason that “growth was good” is that it fueled Facebook’s business model as data broker.

321. Numerous internal Facebook employees and investors voiced privacy concerns to Mr. Zuckerberg and others.

322. For instance, Facebook’s operations manager, Sandy Parakilas, objected to how Facebook handled privacy concerns arising from Graph API v.1.0. He was concerned that Facebook never audited any app developers using Facebook’s Graph API v.1.0 as of 2010, and he raised his concerns about the data vulnerabilities on Facebook Platform to Facebook executives.<sup>121</sup> Parakilas was also concerned that when developers violated Facebook’s Data Use

---

<sup>120</sup> *Id.*

<sup>121</sup> Digital, Culture, Media and Sport Committee (House of Commons), Examination of Witness Sandy Parakilas at Q1191-194, Mar. 21, 2018, <http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/digital-culture-media-and-sport-committee/fake-news/oral/80809.html>.

Policy, Facebook users were (to the best of his knowledge) never notified that developers had inappropriately accessed their data.<sup>122</sup>

323. In a *New York Times* op-ed, Parakilas wrote of the reaction he received from executives after he raised privacy concerns about Graph API v.1.0:

[W]hen I was at Facebook, the typical reaction I recall looked like this: try to put any negative press coverage to bed as quickly as possible, with no sincere efforts to put safeguards in place or to identify and stop abusive developers. When I proposed a deeper audit of developers' use of Facebook's data, one executive asked me, "Do you really want to see what you'll find?" The message was clear: The company just wanted negative stories to stop. It didn't really care how the data was used.<sup>123</sup>

324. Indeed, an executive at Facebook "advised [Parakilas] against looking too deeply at how the data was being used." Facebook, Parakilas has commented, "felt that it was better not to know."<sup>124</sup>

325. Likewise, in October 2016, Roger McNamee (an early investor in Facebook) sent a draft of an op-ed outlining security risks of election interference on Facebook to Mr. Zuckerberg and Ms. Sandberg ahead of publishing. According to Mr. McNamee:

They each responded the next day. The gist of their messages was the same: We appreciate you reaching out; we think you're misinterpreting the news; we're doing great things that you can't see. Then they connected me to Dan Rose, a longtime Facebook executive with whom I had an excellent relationship. Dan is a great listener and a patient man, but he was unwilling to accept that there might be a systemic issue. Instead, he asserted that Facebook was not a media company, and therefore was not responsible for the actions of third parties.

326. And in 2017, Alex Stamos, Facebook's then-Chief of Security, authored a white paper that was later scrubbed for mentions of Russia. On October 19, 2017, ZDNet reported on a leaked recording of an internal Facebook meeting held in late July 2017. In the recording, Mr. Stamos raised security privacy concerns, stating, "We have made intentional decisions to give

---

<sup>122</sup> *Id.* at Q1200-201.

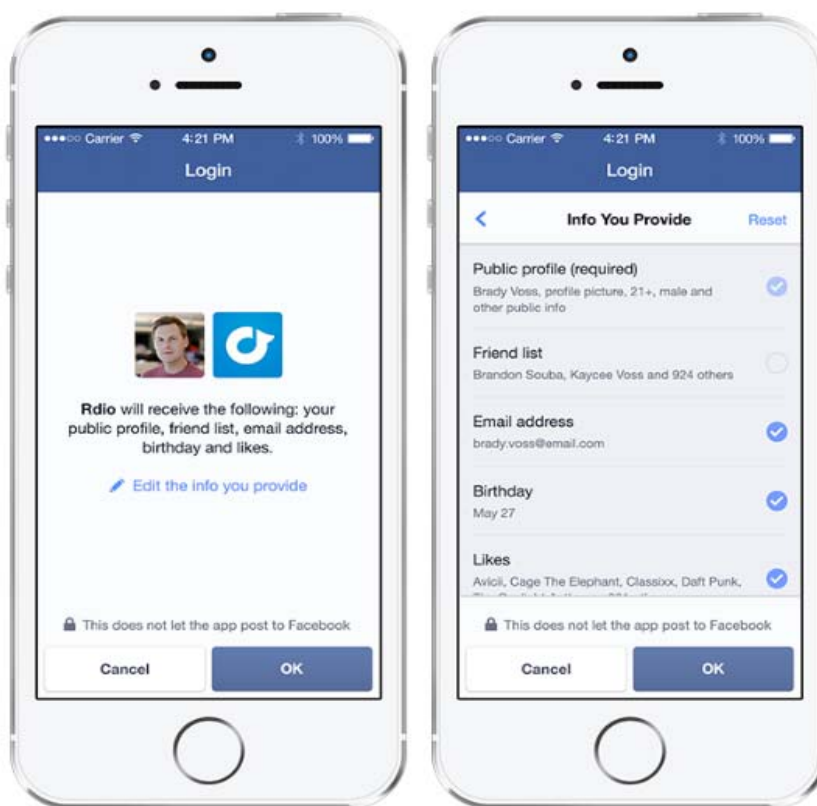
<sup>123</sup> Sandy Parakilas, *We Can't Trust Facebook to Regulate Itself*, N.Y. Times (Nov. 19, 2017), <https://www.nytimes.com/2017/11/19/opinion/facebook-regulation-incentive.html>.

<sup>124</sup> *Id.*

access to data and systems to engineers to make them ‘move fast’ but that creates other issues for us.” Facebook now admits that it was too slow to act with regards to this issue.

### 3. Facebook’s Failure to Implement Reasonable Security Measures

327. Facebook recognized the need for a new login feature that would allow users more control over their settings; however, they failed to implement these changes in a timely manner. On April 30, 2014, at the f8 Developers Conference, Facebook announced new changes to its login system for third-party apps. The first change Facebook announced was a new login for mobile apps that “now offer[] users more fine-grained controls over what they share with an app.” Pictured below:



328. This new login system seemingly gave users fine-grained control over what they shared with app developers. Facebook’s stated about this feature: “Click Log in with Facebook on many apps and you should see the usual permission window open, only now you should see a link that says ‘Edit the info you provide.’ Clicking this will bring up a list of permissions the app is requesting. You will see check marks beside each line of permission. Many of these are

actually optional, and you can now uncheck them to prevent that specific information from being shared. Also, by default, apps will no longer be able to post to Facebook on your behalf. You will need to approve this when you first connect to the app.”<sup>125</sup>

329. Facebook did not require existing applications to switch to this new feature until April 30, 2015. This feature did not change the settings for users who were already logged into an app. If users had already logged in, there was no way to go and delete data they may have passed on to third-party developers.

330. Also in April 2014, Zuckerberg announced a new anonymous login feature for users.<sup>126</sup> This feature would allow users to try an app without sharing any content and



information.

<sup>125</sup> Editor, *New Facebook Account Login Features*, TechAdvisory (July 22, 2014), <http://www.techadvisory.org/2014/07/new-facebook-account-login-features/>.

<sup>126</sup> Referring to the blue Facebook login button, Mr. Zuckerberg stated: “We know some people are scared of pressing this blue button. It’s some of the most common feedback we get on our platform . . . .” Josh Constance, *Facebook Launches Anonymous Login So You Can Try Apps Without Giving Up Your Data*, TechCrunch (Apr. 30, 2014), <https://techcrunch.com/2014/04/30/facebook-anonymous-login/>.

331. This anonymous login feature was never taken out of development. On May 2015, Eddie O’Neil, product manager for Facebook’s login products stated, “Only a ‘couple dozen’ app developers have access to the tool, and fewer than a dozen are actually using it as part of their app.”<sup>127</sup> Facebook later confirmed that it killed the project in August 2015, “due to lack of interest from developers,” even though this app feature would have helped users limit the amount of information that apps could receive.<sup>128</sup>

332. Facebook announced its plans to add a “Clear History” option that will:

[E]nable people to see the websites and apps that send us information when they use them, delete this information from their accounts, and turn off our ability to store it associated with their accounts going forward. . . . If a user clears his or her history or uses the new setting, we’ll remove identifying information so a history of the websites and apps the user used won’t be associated with the user’s account. We’ll still provide apps and websites with aggregated analytics—for example, we can build reports when we’re sent this information so we can tell developers if their apps are more popular with men or women in a certain age group. We can do this without storing the information in a way that’s associated with the user’s account, and as always, we don’t tell advertisers who a user is.”<sup>129</sup>

333. Facebook claimed in May it would release this feature “in the coming months,” but has not as of this filing.<sup>130</sup>

334. Moreover, and prior to April 4, 2018, people, including non-Facebook users, could enter another person’s phone number or email address into Facebook search to help find them. Facebook recently reported that it would be removing this feature:

[M]alicious actors have . . . abused these features to scrape public profile information by submitting phone numbers or email addresses they already have through search and account recovery. Given the scale and sophistication of the activity we’ve seen, we believe most people on Facebook could have had their public profile scraped in this way.

---

<sup>127</sup> Kurt Wagner, *Whatever Happened to Facebook’s Anonymous Login?*, Recode (Mar. 6, 2015), <https://www.recode.net/2015/3/6/11559878/whatever-happened-to-facebooks-anonymous-login>.

<sup>128</sup> *Id.*

<sup>129</sup> Letter from Facebook, Inc. to Chairman Greg Walden, Ranking Member Frank Pallone, Energy & Commerce Committee, and U.S. House of Representatives, *Facebook’s Response to House Energy and Commerce Questions for the Record* (June 29, 2018) at DeGette § 10 ¶ 3.

<sup>130</sup> Chris Welch, *Facebook to Introduce Clear History Privacy Tool in Coming Months*, Verge (May 1, 2018), <https://www.theverge.com/2018/5/1/17307346/facebook-clear-history-new-privacy-feature>.



So we have now disabled this feature. We're also making changes to account recovery to reduce the risk of scraping as well.

**4. Facebook's Failure to Notify Plaintiffs and Class Members of the Misuse of Their Data Made Remedial Measures Impossible**

335. Despite Facebook's actual knowledge that Class Members' content and information had been collected and used without their authorization, and that such misuse of Class Members' data presented substantial risk of further misuse, fraud, and other identity theft to Class Members, and despite assuring its users that privacy and trust were important parts of Facebook's service, Facebook deliberately failed to provide notification to Class Members of the misuse of their content and information without and/or in excess of authorization, until March 2018—approximately three years after it was informed of the Cambridge Analytica Scandal.

336. In the intervening years between 2015, when the *Guardian* notified Facebook of the release of content and information to Cambridge Analytica, and 2018, when Facebook admitted, after further reporting, that this had occurred, Facebook failed to inform Plaintiffs and Class Members that their sensitive content and information had been used without and/or in excess of their authorization and denied them the opportunity to take steps to protect themselves and mitigate their heightened risk of identity theft and other harms.

337. Plaintiffs and Class Members were therefore blindsided when they learned that their content and information had been accessed without and/or in excess of their authorization, and was allegedly used by Cambridge Analytica to create targeted advertising on behalf of President Donald J. Trump's 2016 Presidential campaign.

**5. The Cambridge Analytica Scandal Has Triggered Additional Revelations About Misuse of User Data**

338. Following the Cambridge Analytica Scandal, Facebook conducted its own internal audit into other app developers, but has not made the details public, with scant exception. Audit reports prepared by PriceWaterhouseCoopers have been heavily redacted. Nonetheless, it is known that millions of apps had access to users' data prior to Facebook's 2014 platform changes. Facebook has now admitted that it has suspended 400 of them "due to concerns around the developers who built them or how the information people chose to share

with the app may have been used.” Facebook’s review is limited to apps that had access prior to 2014, when Facebook changed its platform policies. However, reports continue to emerge regarding abuse of user content and information even after this platform change.

339. Facebook has admitted that the Cambridge Analytica Scandal breached its agreements with its users. On March 21, 2018, Mr. Zuckerberg posted to his Facebook account to acknowledge a “breach of trust between Facebook and the people who share their data with us and expect us to protect it” and said, “We need to fix that.” His post stated that in addition to investigating Cambridge Analytica, Facebook was also investigating “all apps that had access to large amounts of information.”

340. Mr. Zuckerberg repeated the same sentiment in full-page ads in several British and American newspapers a few days later. Facebook made these statements to assuage public outcry and prevent users from leaving the platform, as well as to assure regulators. Attempts to distance itself from these statements when called to account in this lawsuit should not be countenanced.

341. Also on March 21, 2018, Sheryl Sandberg posted to her Facebook account that Facebook is “taking steps to reduce the data [Facebook users] give an app” when they use their Facebook account, and the Company intends to “make it easier” for users to have a better understanding of which apps they have “allowed to access [their] data.”

342. On or about April 6, 2018, Facebook suspended AggregateIQ, who played a pivotal role in the Brexit campaign, from the platform, following reports it may be connected to Cambridge Analytica’s parent company, SCL. This was nearly three years after Facebook learned of Cambridge Analytica’s psychographic marketing.

343. On or about April 8, 2018, Facebook suspended the CubeYou app from the platform after CNBC notified them that CubeYou was collecting information about users through quizzes, similar to Cambridge Analytica, and had business ties to Cambridge Analytica.

#### **H. Statements by Facebook’s CEO Give Rise to a Duty to Disclose and Admit to Injury From Lack of Disclosure**

344. Defendant Zuckerberg exerts immense personal control over the direction and

decisions of the Company. When Facebook staged its initial public offering six years ago, it implemented a dual-class share structure that allows Zuckerberg to personally control a majority of the voting stock even though other investors own the majority of the financial value of the company. As a controlled company, Facebook is exempt from certain investor protections in exchange for making detailed disclosures about the fact that if you buy Facebook stock, you are buying into a controlled enterprise.

345. Zuckerberg wrote an Op-Ed in the *Washington Post* in May 2010, outlining the “principles under which Facebook operates” respecting privacy and users’ content and information. “You have control over how your information is shared. We do not share your personal information with people or services you don’t want. We do not give advertisers access to your personal information. We do not and never will sell any of your information to anyone.”<sup>131</sup>

346. On May 27, 2010 Zuckerberg made statements about app developers being required to respect users’ “privacy settings” that gave rise to a duty to inform Plaintiffs and Class Members about the full extent to which app developers and other third parties were able to access their personal content notwithstanding privacy settings: “There’s this false rumor that’s been going around which says that we’re sharing private information with applications and it’s just not true. The way it works, is ... if you choose to share some information with everyone on the site, that means that any person can go look up that information and any application can go look up that information as well. ... But applications have to ask for permission for anything that you’ve set to be private.”<sup>132</sup> These statements also required Facebook to disclose the risks that Facebook would be unable to secure content and information that was shared with third parties.

347. But Zuckerberg went on, making statements give rise to the duty to disclose that

---

<sup>131</sup> Mark Zuckerberg, *From Facebook, Answering Privacy Concerns with New Settings*, Wash. Post (May 24, 2010), <http://www.washingtonpost.com/wp-dyn/content/article/2010/05/23/AR2010052303828.html>.

<sup>132</sup> Mark Memmot, *Zuckerberg: Sharing Is What Facebook Is About*, NPR All Things Considered (May 27, 2010), <https://www.npr.org/sections/alltechconsidered/2010/05/27/127210855/facebook-zuckerberg-privacy>.

Facebook allowed Plaintiffs and Class Members to be targeted by advertisers and marketers that combined their content and information with other data in order to target them: “Advertisers never get access to your information. We never sell anyone's information and we have no plans to ever do that in the future. Now, in order to run a service like this that serves more than 400 million users, it does cost money ... so we do have to make money and the way we do that is through ... advertising. Advertisers come to us and they say what they want to advertise and we show advertisements to people who we think are going to be most interested. ... But at no part in that process is any of your information shared with advertisers.”<sup>133</sup>

348. Zuckerberg created the illusion of security for personal content shared by Plaintiffs and Class Members. Creating “Zuckerberg’s Law,” Zuckerberg built user base and a platform that was designed to encourage users to share more and more content and information: “I would expect that next year, people will share twice as much information as they share this year, and next year, they will be sharing twice as much as they did the year before, he said. “That means that people are using Facebook, and the applications and the ecosystem, more and more.”<sup>134</sup>

349. Zuckerberg created this false sense of security by stressing that while Facebook was built on sharing, it “encouraged” privacy. On June 2, 2010, Zuckerberg stated at a D8 conference: “Privacy is very important to us. I think there are some misperceptions. People use Facebook to share and to stay connected. You don’t start off on Facebook being connected to your friends, you’ve got to be able to find them. So having some information available broadly is good for that. Now, there have been misperceptions that we’re trying to make all information open, but that’s false. We encourage people to keep their most private information private.”<sup>135</sup> Facebook did not disclose that default settings were precisely the opposite of what Zuckerberg

---

<sup>133</sup> *Id.*

<sup>134</sup> Saul Hansell, *Zuckerberg’s Law of Information Sharing*, N.Y. TIMES (Nov. 6, 2008), <https://bits.blogs.nytimes.com/2008/11/06/zuckerbergs-law-of-information-sharing/>

<sup>135</sup> David Catacchio, *Zuckerberg at D8: ‘we recommend privacy settings, we did not change any settings*, TNW website (Jun. 2, 2010), <https://thenextweb.com/socialmedia/2010/06/03/zuckerberg-at-d8-we-recommend-privacy-settings-we-did-not-change-any-settings/>.

described. A trove of content and information that was the most private and intimate to Plaintiffs and Class Members—such as photographs, videos, “likes,” and “status updates”—were by default set to be disclosed by app developers through their friends. Facebook also failed to tell users that the content and information shared with their friends would be accessed by device makers.

350. Zuckerberg also made control of content and information by Plaintiffs and Class Members a foundational pledge. He stated on his Facebook page on November 29, 2011 that “I founded Facebook on the idea that people want to share and connect with people in their lives, but to do this everyone needs complete control over who they share with at all times. ... This idea has been the core of Facebook since day one. When I built the first version of Facebook, almost nobody I knew wanted a public page on the internet. That seemed scary. But as long as they could make their page private, they felt safe sharing with their friends online. Control was key. With Facebook, for the first time, people had the tools they needed to do this. That’s how Facebook became the world’s biggest community online. We made it easy for people to feel comfortable sharing things about their real lives . . .”<sup>136</sup>

351. Following the FTC investigation in 2011, Zuckerberg in the same November 2011 Facebook post doubled down on his promise of privacy and security of content and information: “[G]iving you tools to control who can see your information and then making sure only those people you intend can see it... . As a matter of fact, privacy is so deeply embedded in all of the development we do that every day tens of thousands of servers worth of computational resources are consumed checking to make sure that on any webpage we serve, that you have access to see each of the sometimes hundreds or even thousands of individual pieces of information that come together to form a Facebook page. ... We do privacy access checks literally tens of billions of times each day to ensure we’re enforcing that only the people you want see your content. These privacy principles are written very deeply into our code.”<sup>137</sup> Facebook did not give Plaintiffs and

---

<sup>136</sup> Mark Zuckerberg, *Our Commitment to the Facebook Community*, Facebook, (Nov. 29, 2011), <https://www.facebook.com/notes/facebook/our-commitment-to-the-facebook-community/10150378701937131/>.

<sup>137</sup> *Id.*

Class Members the “tools” they needed to prevent their information from being shared to app developers, device makers, and other third parties.

352. After a report of U.S. government surveillance surfaced in 2014, Zuckerberg reiterated Facebook’s commitment to securing content and information, even though he was aware that Facebook had refused to perform audits as recommend by its executives with oversight responsibilities over third party app developers: “To keep the internet strong, we need to keep it secure. That’s why at Facebook we spend a lot of our energy making our services and the whole internet safer and more secure. We encrypt communications, we use secure protocols for traffic, we encourage people to use multiple factors for authentication and we go out of our way to help fix issues we find in other people’s services. . . . Unfortunately, it seems like it will take a very long time for true full reform. So it’s up to us -- all of us -- to build the internet we want. Together, we can build a space that is greater and a more important part of the world than anything we have today, but is also safe and secure.”<sup>138</sup>

353. Zuckerberg began 2018 by admitting that Facebook had failed to protect Plaintiffs and Class Members’ content and information: “The world feels anxious and divided, and Facebook has a lot of work to do -- whether it’s protecting our community from abuse and hate, defending against interference by nation states, or making sure that time spent on Facebook is time well spent. My personal challenge for 2018 is to focus on fixing these important issues. We won’t prevent all mistakes or abuse, but we currently make too many errors enforcing our policies and preventing misuse of our tools.”<sup>139</sup>

354. When the Cambridge Analytica Scandal broke in March 2018, Zuckerberg admitted that this revelation demonstrated that Facebook had failed to secure Plaintiffs’ and Class Members’ content and information: “This was clearly a mistake. We have a basic responsibility to protect people’s data, and if we can’t do that then we don’t deserve to have the

---

<sup>138</sup> Mark Zuckerberg, FACEBOOK (Mar. 13, 2014), <https://www.facebook.com/zuck/posts/10101301165605491>.

<sup>139</sup> Mark Zuckerberg, FACEBOOK (Jan. 4, 2018), <https://www.facebook.com/zuck/posts/10104380170714571>.

opportunity to serve people.”<sup>140</sup>

355. Zuckerberg has publicly claimed responsibility for Plaintiffs’ and Class Members’ privacy on the Facebook platform when Zuckerberg testified before Congress in April 2018: “We didn’t take a broad enough view of our responsibility, and that was a big mistake,” Zuckerberg’s testimony continued. “It was my mistake, and I’m sorry. I started Facebook, I run it, and I’m responsible for what happens here.” Zuckerberg’s statements conceded that Facebook had failed to fulfill its promise that Facebook users owned and controlled their content and information: “It’s not enough to just give people control over their information, we need to make sure that the developers they share it with protect their information too.”<sup>141</sup>

356. In the wake of the Cambridge Analytica Scandal, Facebook admitted that its current disclosures and privacy settings were confusing and ineffective. Facebook stated in a blog post in March 2018 that “The last week showed how much more work we need to do to enforce our policies, and to help people understand how Facebook works and the choices they have over their data. ... We’ve heard loud and clear that privacy settings and other important tools are too hard to find, and that we must do more to keep people informed.”<sup>142</sup>

**I. Facebook’s Cultivation and Release of Its Users’ Data Were Part of a Lucrative Market for Big Data Where Users’ Content and Information is Valuable, Marketable Property**

**1. Facebook Has Generated Significant Revenue from Allowing Access to Its Users’ Content and Information**

357. As just discussed, Facebook enabled third-party app developers and device

---

<sup>140</sup> Danielle Wiener-Bronner, *Mark Zuckerberg Has Regrets: ‘I’m Really Sorry That This Happened’*, CNN Tech (Mar. 21, 2018), <http://money.cnn.com/2018/03/21/technology/mark-zuckerberg-apology/index.html>; Mark Zuckerberg in his own words: The CNN interview, CNN Tech, Mar. 21, 2018, <http://money.cnn.com/2018/03/21/technology/mark-zuckerberg-cnn-interview-transcript/>.

<sup>141</sup> *Facebook CEO Mark Zuckerberg Hearing on Data Privacy and Protection*, C-SPAN (Apr. 10, 2018), <https://www.c-span.org/video/?443543-1/facebook-ceo-mark-zuckerberg-testifies-data-protection> (complete opening statement in Senate Hearing).

<sup>142</sup> Arjun Kharpal, *Facebook rolls out its first changes since Mark Zuckerberg promised to ‘do better’*, CNBC (Mar. 28, 2018), <https://www.cnbc.com/2018/03/28/facebook-unveils-new-privacy-tools-to-let-you-control-your-data-better.html>.



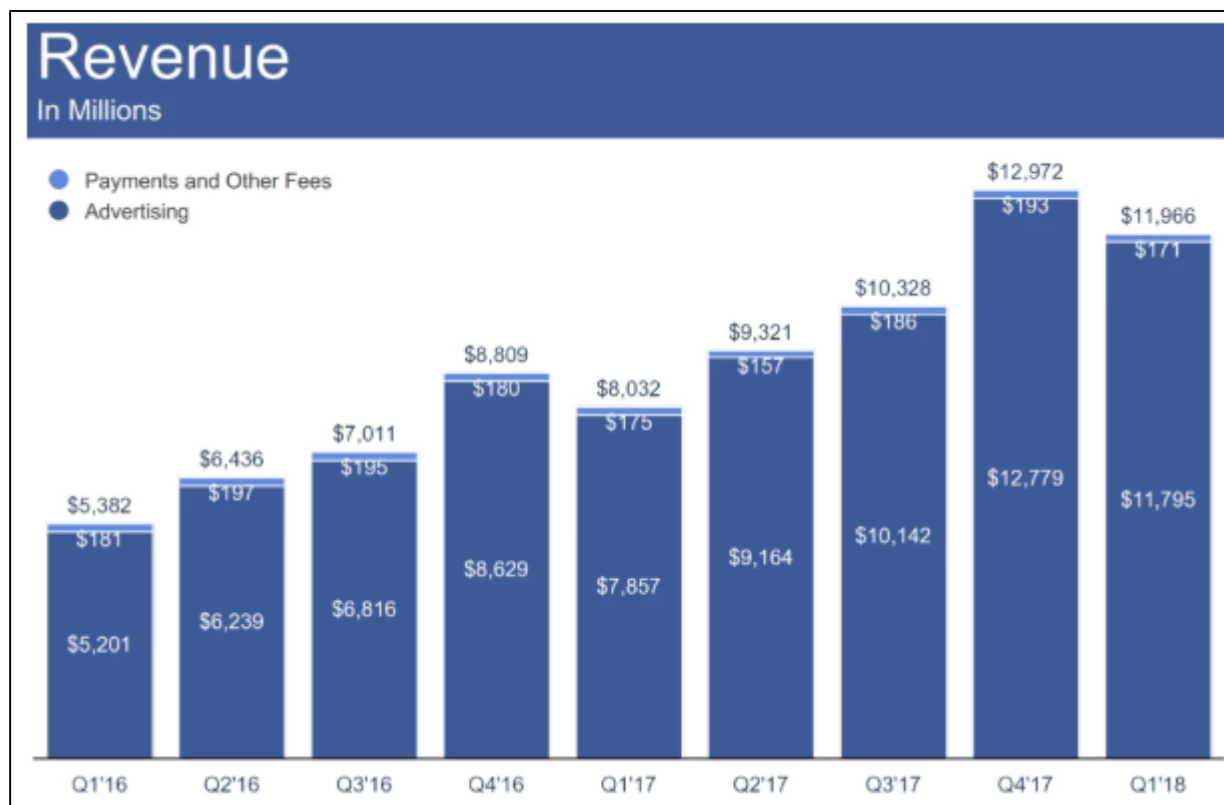
makers to have access to millions of users' content and information. It did so because selling access is how it makes money. Facebook has invested in some of these apps as well, subsequently acquiring them, or retaining a percentage of the apps' earning. Thus the growth of apps fuels Facebook's growth.

358. Critical to this story was the wild success of the app Farmville, which Facebook launched in 2009. A "farming solution social game," Farmville became the most popular game on Facebook's site and stayed that way for nearly two years. Developed by Zynga, which Facebook later acquired, Farmville was a firehouse of user content and information for Facebook, jumpstarting Facebook's aggressive move into data brokering.

359. Collecting data about Facebook users (and non-users) is simply the means to an end in one of Facebook's largest revenue streams. Indeed, for its first quarter 2018 earnings, Facebook reported \$11.97 billion in revenue and \$4.98 billion in profit for the past quarter, with advertising accounting for most of the company's revenue.<sup>143</sup>

---

<sup>143</sup> Emil Protalinski, *Over 90% of Facebook's Advertising Revenue Now Comes From Mobile*, Venture Beat (Apr. 25, 2018), <https://venturebeat.com/2018/04/25/over-90-of-facebooks-advertising-revenue-now-comes-from-mobile/>.



360. The data Facebook has now collected is extremely valuable. Facebook shares those digital profiles with app makers in exchange for buying advertising, and in exchange for further information about the users—what games they like to play, how much time they spend playing what game, how good they are, etc. The information is intimate. Facebook does not fully disclose to the users themselves what information and content it has collected about them. There is no opportunity to prevent the sharing of that aggregated profile or to correct it. For many of the app developers who charge, Facebook retains a portion of their revenues.

## 2. Facebook Has Gained This Revenue by Acting as a Data Broker—and Partnering with Other Data Brokers

361. Including Facebook, there are between 2,500 to 4,000 data brokers in the United States. One of the largest of these is Facebook. The information that these brokers collect includes government identification numbers, biometrics (body measurements and calculations such as facial recognition), account numbers, purchase histories, mother's maiden name, data and place of birth, Social Security numbers, social preferences, political viewpoints, connections,

etc. Bundled together, this information effectively commoditizes individuals' identities, becoming the digital equivalent of a person's existence.

362. Data brokers are notoriously secretive, in part because they want consumers to remain unaware of the many ways in which they are surveilled. Large data brokers collect content and information and consolidate it into virtual profiles of individuals, doing so primarily for four purposes: marketing and predictive analytics; people-search functions; risk mitigation; and predictive voting models. None of these purposes directly serves the ends of the people about whom this content and information is gathered. Marketing and predictive analysis and predictive voting models are used to trigger response and action in the users whose content and information has been collected to benefit those seeking to sell votes or products. Even the risk mitigation purpose, ostensibly to weed out fraud, does not do so from the perspective of preventing individuals from identity theft, for example. Rather, it is used to protect entities purchasing aggregated content and information to prevent fraud to them.

363. Adweek reported in April 2013 that Facebook had partnered with data broker firms such as Datalogix "to find out how the social network influences online purchasing behavior." Through these partnerships Facebook could "tell what users have purchased, even when they're not on the site. It's a way for Facebook to show advertisers that users can and do make purchases after seeing or engaging with an ad on" Facebook.

364. To assess the impact of Facebook advertisements on shopping in the physical world, Datalogix provides Facebook with dataset that includes hashed email addresses, hashed phone numbers, and Datalogix ID numbers for everyone they are tracking. Using the information Facebook already has about its own users, Facebook tests various email addresses and phone numbers against the dataset until it has a long list of the Datalogix ID numbers associated with different Facebook users. By matching the information provided by data brokers with the content and information that Facebook curates on its platforms, including its apps, Facebook has created and maintains digital dossiers of millions of individuals. These dossiers include names, addresses, health information, information about your neighbors, inclinations, proclivities. All of

these are used to predict future behavior, as described below. In consenting to use Facebook, users did not and could not have imagined that they could be so surveilled. Indeed, a March 2018 study showed 70% of Facebook users did not think their data was being collected when they were off Facebook. This is a painfully wrong belief.

365. To aggregate and match user data, Facebook forged relationships with the following data brokers:

- Acxiom, which can provide data from Australia, France, Germany, the UK and the US;
- Acxiom Japan, which can provide data from Japan;
- CCC Marketing, which can provide data from Japan;
- Epsilon, which can provide data from the US;
- Experian, which can provide data from Australia, Brazil, the UK and the US;
- Oracle Data Cloud (formerly Datalogix), which can provide data from the UK and the US; and
- Quantum, which can provide data from Australia.

366. Facebook worked with these data brokers to collect information about consumers through public records, loyalty card programs, surveys, and independent data providers. In 2016 ProPublica reported that Facebook collects more than 52,000 unique data points to classify users. According to the article, Facebook provided at least 29,000 targeted categories for advertisers to choose from. Nearly 600 of these categories were provided by third-party data brokers.

367. Facebook has not informed users that it matches content and information users reveal on the Facebook platform with information provided through data brokers collected from a myriad of sources to build digital profiles of them. While some data brokers, like Acxiom, have allow consumers to review and correct their profiles, Facebook does not.<sup>144</sup> Facebook users have not been informed these exist, let alone have the opportunity to review or correct those profiles. As even Acxiom notes, transparency is key to maintain user trust.

---

<sup>144</sup> Natasha Singer, *Acxiom Lets Consumers See Data It Collects*, N.Y. Times (Sept. 4, 2013), <https://www.nytimes.com/2013/09/05/technology/acxiom-lets-consumers-see-data-it-collects.html>.

**J. The Content and Information About Its Users That Facebook Has Shared With Third Parties Has Allowed Advertisers and Political Operatives to Harass and Discriminate Against Them**

**1. Facebook Users Did Not Understand that Their Content and Information Would Be Used for Psychographic Marketing**

368. Facebook users did not understand and would have behaved differently if they understood how their content and information would be collected and then used for a special kind of targeted messaging called “psychographic marketing.” Politicians, advertisers and even foreign nations all engaged in psychographic marketing on Facebook and using user content and information that had been disclosed to third parties without users’ authorization.

369. Psychographic marketing exploits a Facebook user’s fears, feelings, and values. Psychographic marketing appeals to a person’s motives and instincts—focusing on why a consumer makes the decisions that she does—in order to influence emotion, mood, and behavior.

370. Psychographic tendencies can be determined by a person’s reaction to polarizing issues, and can be measured and monetized on a platform like Facebook like perhaps, on a mass level, no other way in human history. “The psychographic identities that develop and deepen online can erupt into active conflict between groups, which provides both opportunities and challenges for marketers. Conflicts can help you identify key psychographics: the Facebook arguments between pro- and anti-screen parents inspired my research into parents’ tech attitudes. But conflicts can also make it difficult to speak to your audience, since a marketing strategy that extolls the play value of a tech device would turn off some parents, while delighting others. That’s exactly why psychographic data is so essential: it gives you a roadmap for navigating these types of divisions and sensitivities.”<sup>145</sup>

371. Cambridge Analytica used psychographic marketing techniques to predict a person’s political views using content and information provided by Facebook. Cambridge Analytica “harvest[ed] the Facebook profiles of millions of people in the United States, and to use their private and personal content and information to create sophisticated psychological and

---

<sup>145</sup> Alexandra Samuel, *Psychographics Are Just as Important for Marketers as Demographics*, Harv. Bus. Sch. (Mar. 11, 2016), <https://hbr.org/2016/03/psychographics-are-just-as-important-for-marketers-as-demographics>.

political profiles. And then target them with political ads designed to work on their particular psychological makeup.”<sup>146</sup> “Christopher Wylie, the former [Cambridge Analytica] employee who recently came forward to detail how the company improperly acquired personal data from fifty million Facebook users, has said that the company used that data to create a ‘psychological warfare mindfuck tool.’”<sup>147</sup>

372. Psychographic marketing, to be successful, de-anonymizes its audience, and invades an audience’s privacy by pinpointing personality traits for manipulation and deeply exploiting deeply-ingrained values and beliefs. According to Alexander Nix:

[W]e [were] able to commercially acquire large datasets on citizens across the United States—on adults across the United States—that comprise of consumer and lifestyle data points. This could include anything from their hobbies to what cars they drive to what magazines they read, what media they consume, what transactions they make in shops and so forth. . . . “I think I have made my position clear, which is that we are trying to make sure that we can use data to understand what people care about . . . .”<sup>148</sup>

373. Cambridge Analytica developed detailed voting profiles for U.S. and U.K. voters and used this information to enhance psychographic marketing techniques. Cambridge Analytica had information such as names, addresses, date of birth, and voter registration information for U.S. voters. It also had individual voter results. It also had a political profile that was comprised of ten variables, ranked in order of perceived importance, as well as the likely vote in the 2016 presidential election.

374. Cambridge Analytica used psychographic models to direct messages to U.S. voters. Alexander Nix stated that the voter profiles were used to “micro target” individual

---

<sup>146</sup> Carole Cadwalladr, *‘I Made Steve Bannon’s Psychological Warfare Tool’: Meet the Data War Whistleblower*, Guardian (Mar. 18, 2018), <https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-facebook-nix-bannon-trump>.

<sup>147</sup> Sue Halpern, *Cambridge Analytica and the Perils of Psychographics*, New Yorker (Mar. 30, 2018), <https://www.newyorker.com/news/news-desk/cambridge-analytica-and-the-perils-of-psychographics>.

<sup>148</sup> Statement of Claimant ¶ 20(f), *Carroll v. Cambridge Analytica Ltd.* [2018] EWHC (QB) (Eng.).

voters.<sup>149</sup> Cambridge Analytica used Plaintiffs' content and information to run "4,000 different advertising campaigns—about 1.4 billion impressions."<sup>150</sup> Much of this was on Facebook.

375. According to David Carroll, Professor at the Parsons School of Design in New York City:

[Cambridge Analytica] claim to have figured out how to project our voting behavior based on our consumer behavior. So it's important for citizens to be able to understand this because it would affect our ability to understand how we're being targeted by campaigns and how the messages that we're seeing on Facebook and television are being directed at us to manipulate us. ... I think it is a matter of the relationship between privacy and democracy.<sup>151</sup>

376. The Cambridge Analytica Scandal and subsequent investigations have revealed that it was not just Kogan and Cambridge Analytica that purchased Facebook user content and information with the goal of manipulating them. Psychographic marketing is the preferred method of targeted advertising, and consumer data like Facebook user and content is its oil.<sup>152</sup>

## **2. The Features That Facebook Has Offered Advertisers Allow Extraordinarily Harmful and Invasive Forms of Psychographic Marketing**

377. Starting in 2012, Facebook released its "Custom Audiences" feature, which allows advertisers to directly target specific Facebook users with advertisements.

378. One way that advertisers can target a Custom Audience of Facebook users is by uploading a spreadsheet with Facebook user identifying information, including Email, Phone Number, Mobile Advertiser ID, First Name, Last Name, Zip/Postal Code, City, State/Province, Country, Date of Birth, Year of Birth, Gender, Age, Facebook App User ID, and Facebook Page

---

<sup>149</sup> *Id.* ¶ 20(h)

<sup>150</sup> *Id.*

<sup>151</sup> Brent Bambury, *Data Mining Firm Behind Trump Election Built Psychological Profiles of Nearly Every American Voter*, CBC Radio (Mar. 20, 2018), <https://www.cbc.ca/radio/day6/episode-359-harvey-weinstein-a-stock-market-for-sneakers-trump-s-data-mining-the-curious-incident-more-1.4348278/data-mining-firm-behind-trump-election-built-psychological-profiles-of-nearly-every-american-voter-1.4348283>.

<sup>152</sup> Mark Andrus, *The New Oil: The Right to Control One's Identity in Light of the Commoditization of the Individual*, Bus. Law Today (Sept. 28, 2017), <https://businesslawtoday.org/2017/09/the-new-oil-the-right-to-control-ones-identity-in-light-of-the-commoditization-of-the-individual/>.



User ID.

379. Advertisers can also target a Custom Audience of Facebook users based on (a) visitors to a given website, (b) users of a given app or game; (c) people who interacted with a given business offline, such as by visiting or calling a business; and (d) people who engaged with content on Facebook or Instagram, such as by viewing a video on Facebook or Instagram.

380. To be clear, there is nothing problematic with targeted advertising in isolated contexts. But as data has accumulated about users, combined with information obtained from data brokers, a body of information has been accumulated that is available not to the users themselves, but to third parties who make decisions about users' healthcare, finances, insurances, housing and other decisions without users' knowledge. And it is clear that Facebook did not control or audit how these third parties target Facebook users.

381. For example, Facebook's "Managed Custom Audiences" feature "enabled advertisers to access third-party data from approved data providers, like Acxiom and Oracle, through Facebook-managed deals with those providers and then use that data to target their Facebook ads."<sup>153</sup> Facebook's Managed Custom Audiences feature was made possible by its partnerships with data brokers, through which Facebook matched the data it collects about its users and matches this with data collected by its partner data brokers regarding Facebook users. TechCrunch notes that, although Facebook discontinued its Partner Categories program, it "left open the option for businesses to compile illicit data sets or pull them from data brokers, then upload them to Facebook as Custom Audiences by themselves."<sup>154</sup>

382. On August 22, 2018, Facebook confirmed that it has continued to allow advertisers to target Custom Audiences of Facebook users with advertisements based on data obtained from data brokers, stating that it is allowable for "data providers and agencies [to]

---

<sup>153</sup> Tim Peterson, *Facebook Will Remove Advertisers' Other Third-Party Option, But Loopholes, Questions Remain*, DigiDay (Apr. 6, 2018), <https://digiday.com/marketing/facebook-will-remove-advertisers-third-party-data-option-loopholes-questions-remain/>.

<sup>154</sup> John Constine, *Facebook Plans Crackdown on Ad Targeting by Email Without Consent*, TechCrunch (Mar. 31, 2018), <https://techcrunch.com/2018/03/31/custom-audiences-certification/>.

create, upload and then share certain Custom Audiences on behalf of advertisers,” and therefore Facebook is “clarifying [its] terms to make it clear that advertisers can do this—they can independently work with partners off our platform to create Custom Audiences, as long as they have the necessary rights and permissions to do so.”<sup>155</sup> These intrusions into user spaces by outside advertisers based on data accumulated and merged with user data violates Facebook’s promise not to give advertisers’ the content and information of users.

383. Plaintiffs and Class Members did not consent to receiving advertisements targeted directly to them through Facebook’s Managed Custom Audiences or Custom Audiences feature. Until recently, Facebook did not even require advertisers using its Managed Custom Audiences or Custom Audiences feature to accept responsibility for obtaining the “necessary permissions from the people in the audience to use and share their information.” On July 2, 2018, Facebook for the first time started requiring advertisers who wish to target specific Facebook users with advertisements to accept responsibility for obtaining permissions from such users.<sup>156</sup>

384. TechCrunch notes, “Facebook is trusting advertisers to tell the truth about consent for targeting . . . despite them having a massive financial incentive to bend or break those rules,” and, although this new requirement “will give Facebook more plausible deniability in the event of a scandal, and it might deter misuse,” the fact remains that “Facebook is stopping short of doing anything to actually prevent non-consensual ad targeting.”<sup>157</sup>

385. Moreover, despite the Cambridge Analytica Scandal, Facebook *still* does not require its users to provide affirmative consent before allowing advertisers to directly target such users with advertisements through Facebook’s Custom Audiences feature.

---

<sup>155</sup> *Facebook Business: Introducing New Requirements for Custom Audience Targeting*, Facebook, <https://www.facebook.com/business/news/introducing-new-requirements-for-custom-audience-targeting> (last visited Sept. 20, 2018).

<sup>156</sup> Stephen Lam, *Facebook Releases New Privacy Safeguards on How Advertisers Handle Data*, NBC News (June 13, 2018), [https://www.nbcnews.com/tech/social-media/facebook-releases-new-privacy-safeguards-how-advertisers-handle-data-n882781?cid=sm\\_npd\\_nn\\_fb\\_ma](https://www.nbcnews.com/tech/social-media/facebook-releases-new-privacy-safeguards-how-advertisers-handle-data-n882781?cid=sm_npd_nn_fb_ma).

<sup>157</sup> John Constine, *Facebook Demands Advertisers Have Consent for Email/Phone Targeting*, TechCrunch (June 13, 2018), <https://techcrunch.com/2018/06/13/facebook-custom-audiences-consent/>.

386. Using the content and information that Facebook improperly disclosed to app developers, device makers, and others, third parties including Cambridge Analytica directly targeted specific Facebook users with advertisements that would be highly offensive to a reasonable person.

387. The lesson of the Cambridge Analytica Scandal is not that targeted advertising itself is bad. It is that the aggregation of users' content and information, which was obtained without users' consent, is being used in ways that beyond the reasonable expectations of users. Cambridge Analytica sought to "exploit[] essentially mental vulnerabilities in certain types of people in the context of making them vote in a particular way."<sup>158</sup> For instance, "a neurotic, extroverted and agreeable Democrat could be targeted with a radically different message than an emotionally stable, introverted, intellectual one, *each designed to suppress their voting intention*—even if the same messages, swapped around, would have the opposite effect."<sup>159</sup>

388. The aggregated stolen data was used to discriminate. Cambridge Analytica sought targeted African American voters with the goal of suppressing their votes: "Facebook posts were targeted at some black voters reminding them of Hillary Clinton's 1990s description of black youths as 'super predators', in the hope it would deter them from voting."<sup>160</sup>

389. Other examples of discrimination abound. Although not the subject of this lawsuit, claims have been brought against Facebook for permitting advertisers to target them or exclude them. On July 24, 2018, the Washington State Office of Attorney General announced that Facebook signed a legally binding agreement to make changes to its "advertising platform by removing the ability of third-party advertisers to exclude ethnic and religious minorities,

---

<sup>158</sup> Redazione, *Exclusive Interview with Christopher Wylie, the Cambridge Analytica Whistleblower*, Vogue (May 9, 2018), <https://www.vogue.it/en/news/daily-news/2018/05/09/interview-with-christopher-wylie-cambridge-analytica/>.

<sup>159</sup> Alex Hern, *Cambridge Analytica: how did it turn clicks into votes?*, Guardian (May 6, 2018), <https://www.theguardian.com/news/2018/may/06/cambridge-analytica-how-turn-clicks-into-votes-christopher-wylie> (emphasis added).

<sup>160</sup> Olivia Solon, *Cambridge Analytica Whistleblower Says Bannon Wanted to Suppress Voters*, Guardian (May 16, 2018), <https://www.theguardian.com/uk-news/2018/may/16/steve-bannon-cambridge-analytica-whistleblower-suppress-voters-testimony>.

immigrants, LGBTQ individuals and other protected groups from seeing their ads.”<sup>161</sup>

Investigators in the Attorney General’s Office successfully used the platform to create 20 fake ads that excluded one or more ethnic minorities from receiving their advertising for nightclubs, restaurants, lending, insurance, employment and apartment rentals. This meant that these ethnic groups would not be able to see the ads at all, and would therefore be unaware of the opportunities in the advertisements.

For example, AGO investigators posed as a restaurant. The restaurant ad excluded African-American, Asian-American and Latinx ethnic affinity groups.

Despite discriminatory exclusions and language, Facebook’s advertising platform approved all 20 ads.

\* \* \*

- In addition to housing, credit and employment ads, Facebook will no longer provide advertisers with options to exclude ethnic groups from advertisements for insurance and public accommodations. . . .
- Facebook will no longer provide advertisers with tools to discriminate based on race, creed, color, national origin, veteran or military status, sexual orientation and disability status. These exclusion options will not be present on any advertisement for employment, housing, credit, insurance and/or places of public accommodation.<sup>162</sup>

390. On August 13, 2018, the Department of Housing and Urban Development (“HUD”) filed a complaint against Facebook, stating that “Facebook unlawfully discriminates by enabling advertisers to restrict which Facebook users receive housing-related ads based on race, color, religion, sex, familial status, national origin and disability.”<sup>163</sup>

---

<sup>161</sup> *AG Ferguson Investigation Leads to Facebook Making Nationwide Changes to Prohibit Discriminatory Advertisements on its Platform*, Wash. State Office of the Attorney Gen. (July 24, 2018), <https://www.atg.wa.gov/news/news-releases/ag-ferguson-investigation-leads-facebook-making-nationwide-changes-prohibit>.

<sup>162</sup> *Id.*

<sup>163</sup> Housing Discrimination Complaint, *Assistant Sec’y for Fair Hous. & Equal Opportunity v. Facebook, Inc.* (Aug. 13, 2018), [https://www.hud.gov/sites/dfiles/PIH/documents/HUD\\_01-18-0323\\_Complaint.pdf](https://www.hud.gov/sites/dfiles/PIH/documents/HUD_01-18-0323_Complaint.pdf).

391. Regarding Facebook’s practice of discrimination, HUD Assistant Secretary Anna Maria Farias stated, “when Facebook uses the vast amount of personal data it collects to help advertisers to discriminate, it’s the same as slamming the door in someone’s face.”<sup>164</sup>

392. Facebook also faces a suit from the National Fair Housing Alliance over similar practice of allowing advertisers to discriminate based on protected characteristics. *Nat’l Fair Housing Alliance v. Facebook, Inc.*, No. 18-cv-2689 (S.D.N.Y. compl. filed Mar. 27, 2018). The U.S. Attorney for the Southern District of New York has filed a statement of interest supporting this suit.

393. On September 18, 2018, a complaint was filed with the Equal Employment Opportunity Commission alleging that Facebook’s ad filtering function allowed employers to target job advertisements specifically to men. Such a practice excluded women and anyone who identifies as another gender from employment opportunities, according to the complaint.

394. Whistleblower and former Cambridge Analytica director of research Christopher Wylie described Cambridge Analytica’s targeted political advertising as “worse than bullying,” because “people don’t necessarily know it’s being done to them. At least bullying respects the agency of people because they know. So it’s worse, because if you do not respect the agency of people, anything that you’re doing after that point is not conducive to a democracy. And fundamentally, information warfare is not conducive to democracy.”<sup>165</sup>

395. Similarly, Wylie agreed that advertisements placed in a Facebook user’s News Feed are perceived with less scrutiny than traditional political advertisements, “because nobody knows that’s happening—the opposition doesn’t know that’s happening. If it’s also presented to you as a news item, you as the voter don’t know there’s an agenda behind it. If you don’t know who the messenger is, what the agenda is, and you don’t see the other side of something, and you

---

<sup>164</sup> *HUD Files Housing Discrimination Complaint Against Facebook*, HUD (Aug. 17, 2018), [https://www.hud.gov/press/press\\_releases\\_media\\_advisories/HUD\\_No\\_18\\_085](https://www.hud.gov/press/press_releases_media_advisories/HUD_No_18_085).

<sup>165</sup> Carole Cadwalladr, ‘I Made Steve Bannon’s Psychological Warfare Tool’: Meet the Data War Whistleblower, *Guardian* (Mar. 18, 2018), <https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-facebook-nix-bannon-trump>.

keep seeing pieces of information that aren't true or are highly suggestive, and you start making decisions or changing your perception of something—that's deception. That information creates an imbalance of power; you haven't been given to opportunity to see the other side, or to even know why it is that you're seeing that."<sup>166</sup> Users are being targeted with political messaging that they did not authorize and it is not being identified as such.

396. Wylie stated that Cambridge Analytica "specialises in rumour campaigns, and ultimately, disinformation—as a lot of its candidates and clients want that. Cambridge Analytica will set up all kinds of entities and companies which then disappear so no one can trace what they actually do. The way it works is that you set up blogs and news sites—things that don't look like campaign material—and you find people who would be most amenable to this particular conspiracy theory, unfact, 'alternative fact'. You let them start going down the rabbit hole of clicking things. The idea is that you start showing them the same material from all these different kinds of sources, so they feel like they see it everywhere, but they don't see it on the news, on CNN or the BBC. They then question why the 'establishment' doesn't want them to know something."<sup>167</sup> This manipulation was enabled by the aggregation of the users' content and information that Facebook collected and gave to Kogan over a period of years.

397. The information provided by Facebook helped Cambridge Analytica target people in the privacy of their homes. A report by Switzerland's *Das Magazin* revealed that "Trump canvassers were provided with an app allowing them to identify the political views and personality type of a given house, and the outline conversation scripts that would work with the inhabitants."<sup>168</sup>

398. Facebook users deserve clear disclosures about how Facebook is partnering with

---

<sup>166</sup> Redazione, *Exclusive Interview with Christopher Wylie, the Cambridge Analytica Whistleblower*, Vogue (May 9, 2018), <https://www.vogue.it/en/news/daily-news/2018/05/09/interview-with-christopher-wylie-cambridge-analytica/>.

<sup>167</sup> *Id.*

<sup>168</sup> Adam Lusher, *Cambridge Analytica: Who Are They, and Did They Really Help; Trump Win the White House?*, Independent (Mar. 21, 2018), <https://www.independent.co.uk/news/uk/home-news/cambridge-analytica-alexander-nix-christopher-wylie-trump-brexitelection-who-data-white-house-a8267591.html>.

third parties, including advertisers, and what content and information it shares with them.

**3. The Aggregation of User Content Via Third Parties, Including Device Makers and App Developers, Has Greatly Accelerated the Potential for Data Abuse**

399. Facebook sells the opportunity to advertise to its users to third parties who seek to target specific attributes in advertising/lobbying. These attributes include race, gender origination, emotional instability, political viewpoint, financial status, and much more, including the position of your mouse, and data collected through facial recognition technology (“FRT”). The transparency is utterly one way. Users are not told who sponsors ads or news articles that they receive, or what attributes those advertisers were relying upon when they sent the material.

400. Facebook claims that it does not “sell” user data is that it structures transactions so that third parties are paying to advertise. That is, in theory Facebook is maintaining control of the data, and just using it to tailor messages to third parties who want to send to users. The more targeted the advertising, based on this data, the more expensive it is. If a third party, like an advertiser or lobbying group, wishes to target users very specifically, they can narrow the target group so uniquely that it results in a “match”—which is to say, the “anonymized” profile has been matched to the actual person. “Matched” data is much more expensive than just general data, and this has been the source of ever-increasing “average revenue per user,” or ARPU. Facebook reports ARPU to its shareholders and it has increased dramatically since 2014. Average ARPU for US users is \$26/user for 2017. However, each person’s revenue varies with the amount of data collected and it should be able to calculate it at least by region.

401. There is a market for this data, and one of the biggest marketplaces is Facebook. However, now that much of this data has been released, it is also being sold on black markets. A Facebook user profile is estimated to be worth \$1207 on the dark web on average.

**V. PRIMA FACIE CASE OF INJURY AND DAMAGES**

**A. Plaintiffs Suffered Harm as a Direct Result of Facebook’s Conduct**

402. Because Facebook collected and impermissibly shared Plaintiffs’ and Class Members’ content and information with third parties, together with the ability of data brokers



and others to de-anonymize that content and information and link it to specific users, Plaintiffs and Class Members have suffered injuries and will suffer ongoing injuries, which include, but are not limited to (i) loss of benefits in their Facebook experience; (ii) heightened risk of identity theft and fraud; (iii) invasions of privacy; (iv) loss of control of their content and information; (v) out-of-pocket costs; (vi) economic loss; (vii) loss of value of personally identifiable information; (viii) other irreparable loss; and (ix) emotional distress and anxiety.

403. When Plaintiffs and Class Members became Facebook users, users gained access to Facebook's social networking platform in exchange for sharing certain content and information with Facebook, conditioned upon their consent to such sharing. While users knew that Facebook would generate revenue by selling advertising which would be directed to users, it was a material term to the bargain that users were promised control over how and with whom their content and information would be shared.

404. Facebook did not honor the terms of this bargain. Although Facebook told users they owned their data, in practice Facebook acted as if it did. When Facebook, without notice to users, shared users' content and information with third parties that users had not intended to share, Facebook received benefits—revenues associated with increased user activity and sale of additional data generated by the this increase in activity—and transferred costs and harms to Plaintiffs—loss of privacy and control over their valuable content and information.

405. As Facebook expanded the scope of access to users' content and information beyond that to which users had agreed, users were denied the benefit of a Facebook experience where they defined the terms of their content sharing. Thus, through Facebook's actions and inactions, users have lost benefits. In order to preserve their privacy, users were presented with the choice of: (i) reducing their participation on Facebook by limiting the content and information they provide about themselves, (ii) accepting less privacy than that which they were promised; or (iii) ceasing their participation in Facebook altogether. Each of these options resulted in lost value for Plaintiffs and Class Members. The benefits transferred to Facebook had economic gain.

406. Facebook further harmed Plaintiffs and Class Members when it failed to notify users that their content and information could be or had been misappropriated via the Cambridge Analytica Scandal, by its partnerships with device makers, or by other disclosures to third parties. As just one example, following the first revelations of Cambridge Analytica's psychographic profiling in 2015, Facebook failed to take steps to confirm that Cambridge Analytica, and any other entities which had unauthorized possession of users' content and information, had properly deleted users' content and information. Facebook's choice to forego the costs of notification, deletion or other protective action transferred and imposed upon users further costs from the misappropriation. Without the benefit of notification and the ability to prevent future harm, Facebook caused Plaintiffs and Class Members to bear the full burden of the risk of identity theft and fraud, as well as the ongoing imposition of targeted communications, that would be highly offensive to a reasonable person, by third parties in possession of users' content and information.

407. The economic loss to Plaintiffs is real and tangible. The risks of identity theft and fraud are long term and injure users in a multiplicity of ways including: compromising their financial accounts, marring their credit ratings and history, preventing their ability to get loans, risking fraudulent tax filings, the inclusion of misinformation in their medical record leading to improper and dangerous medical treatment, and/or incurring additional costs due to diminishment or loss of insurance coverage, diminishment or loss of employment opportunities and many other potential hardships. Already, Plaintiffs and Class Members have suffered diminished security in their personal affairs and face an expanded and imminent risk of economic harm from identity theft and fraud.

408. Plaintiffs and Class Members face, and Plaintiffs Paige Grays, Jason Ariciu, James Tronka, Barbara Vance-Guerbe have already experienced, additional security risks such as phishing attempts, efforts by hackers trying to access or log in to their Facebook accounts, friend requests from trolls or cloned or imposter accounts, or other interference with their Facebook accounts. The remaining Plaintiffs and Class Members also face these security risks and are

subjected to a heightened risk of such predatory conduct due to Facebook's failure to secure their personal content, including the sale of their users' content and information on the dark web and other illicit databases.

409. Users also suffered diminished loss of use of their own data. There is a market for the content and information that Facebook harvests. By making it ubiquitously available, Facebook has undermined the market value of users' data. One study by content marketing agency Fractl has found that an individual's online identity, including hacked financial accounts, can be sold for \$1200 on the dark web. Facebook logins can be sold for approximately \$5.20 each. These rates are assumed to be discounted because they do not operate in competitive markets, but rather, in an illegal marketplace.

410. Where Plaintiffs and Class Members' content and information is available on the dark web, this imposes further uncompensated costs on those individuals. The dark web permits criminals further access to users' content and information that could potentially allow more serious identity theft or fraud involving an individual's other accounts.

411. Plaintiffs' and Class Members' content and information is aggregated and pooled with other data collected by data brokers, including Facebook, to create digital dossiers or profiles of people. Through "linking" of data from these various sources, users' content and information can be de-anonymized. That multiple data points such as a person's name, address, email address, telephone number and employment history can be matched with other identifying information such as names of pets, grandparents, mother's maiden name, etc. greatly heightens the risk of identity theft and fraud to Plaintiffs and Class Members as well as the economic harms that flow therefrom.

412. Facebook knew that users' content and information was being collected and aggregated in ways that put Plaintiffs and Class Members at heightened risk of identity theft and fraud, and failed to properly inform users of those risks, such that users could reasonably mitigate those potential harms. Rather, Facebook has placed the burden of mitigating the risk of identity theft and fraud on Plaintiffs and Class Members. Following the Cambridge Analytica

Scandal, Facebook offered no support to users who were concerned about the collection of their content and information. In fact, Facebook is still unable to confirm who has possession of Plaintiffs' and Class Members' content and information. As a result, Plaintiffs and Class Members have paid for credit monitoring and have spent time and money to protect themselves from the imminent threat of identity theft and fraud. Dustin Short paid for credit monitoring and to remove inquiries from his credit report in the wake of the revelations about the Cambridge Analytica Scandal. Likewise, Plaintiff Scott McDonnell paid for credit monitoring services. Plaintiffs Forman, Holsinger, O'Hara, and Tronka use credit and bank account monitoring services from multiple providers. These actions were reasonable in light of the scope of content and information Facebook collected, as well as the ability of third parties, with which Facebook impermissibly shared users' content and information, to pool users' Facebook content and information with other data sources and link it to specific Facebook users. As a result, Plaintiffs and Class Members have incurred out-of-pocket costs as a result of Facebook's harmful conduct, including purchasing credit monitoring or other forms of identity theft protection services. Plaintiffs and Class Members have also suffered invasions of their privacy which have resulted in a loss of control of their content and information. Facebook committed an egregious invasion of privacy by publishing and disclosing the content and information of Facebook users to third parties without users' consent, and without advising them of the extent to which it has been disseminated, analyzed and aggregated. Facebook promised users that they could exert control over who could access their content and information and that it would honor their privacy designations.

413. This transfer of costs to users and benefits to Facebook was deliberate. Facebook engineered APIs that enabled third parties to access users' content and information without adhering to users' privacy settings. Moreover, once this data was in the hands of the third parties, Facebook took no steps to prevent its use in ways that were contrary to users' reasonable expectations of privacy. Furthermore, Facebook failed to demand and enforce compliance with its policies by its own app developers, including that user content and information not be sold

and that it be deleted if improperly obtained.

414. In failing to mitigate, Facebook avoided costs it should have incurred as a result of its own actions—both out of pocket and loss of user engagement—and transferred those costs to Plaintiffs and Class Members. Warning Class Members would have chilled user engagement as well as potential new users from joining Facebook. It would also have brought scrutiny on the Company, in the form of transaction costs such as regulatory fines, shareholder concerns, possible executive turnover and a decline in share price. Some of these costs have, of course, materialized. Facebook and CEO Zuckerberg were thus not only able to evade or defer these costs but to continue to accrue value for the Company. Likewise, Facebook further benefited from the delay due to the time value of money. Facebook, as of yet, still has not publicly disclosed the third parties, including app developers, which received access to users' content and information.

415. Plaintiffs suffered egregious invasions of privacy when they were directly targeted by advertisements that would be highly offensive to a reasonable person, and which were enabled by Facebook providing their content and information to unauthorized third parties, who in turn used this content and information in conjunction with other data sources to directly target users using resources provided by Facebook. As a result, Plaintiffs and Class Members experienced, and continue to experience, invasions of privacy and a loss of control of their content and information that endanger their financial, medical and emotional well-being now, and for the rest of their lives.

416. Had Plaintiffs and Class Members known the full extent of the risks that they face because Facebook was disclosing and publishing their content and information to third parties without their consent, and that their data was being analyzed, aggregated and used to de-anonymize other sensitive information and match it to their Facebook identity, and that these disclosures are permanent and irretrievable, users would have taken remedial steps to protect their information and content, even though this further reduced the benefits of their bargain, such as by, (i) reducing, or ceasing altogether, their participation on Facebook by limiting the content

and information they provide about themselves; (ii) knowingly accepting less privacy than that which they were promised. Each of these options would have deprived Plaintiffs of the remaining benefits of the original bargain. Plaintiffs and Class Members were denied the benefit of this information and therefore the ability to mitigate harms they incurred as a result of Facebook's impermissible disclosure and publishing of their content and information.

417. Facebook likewise deceived Plaintiffs and Class Members about its purpose for sharing users' content and information. Facebook falsely stated that personal content was collected to enhance the users' experience, including making purportedly useful apps available to users. Facebook made users' content and information accessible to app developers and other third parties in order to increase Facebook's revenues, doing so in a manner that diminished user value, rather than enhancing it. In many instances, Facebook apps were, in essence, "Trojan horses" that enabled the harvesting of users' content and information. Facebook misled Plaintiffs and Class Members about the fact that it was disclosing, publishing and monetizing their content and information without their knowledge, understanding, or consent. Had Facebook been forthright about its intentions, Plaintiffs and Class Members would have altered their interactions with Facebook as set forth above. *See infra* ¶ 13.

418. Plaintiffs and Class Members also face downstream economic harms from the aggregation of their content and information. There is a fast-growing market for consumer data of this kind. The data is aggregated and analyzed to create "consumer scores" which predict people's propensity to become ill or pay off debt. The World Privacy Forum notes in a lengthy report that major health insurers are looking to collect data about individuals, such as whether "a couple bought hiking boots" or "a woman did a lot of online shopping," in order to "figure out how much to charge people [for healthcare]." As such, the collection and dissemination of this content and information could have a direct effect on something as impactful as how much people pay out-of-pocket for healthcare, resulting in economic harm.

419. Thus, Facebook has transferred all of the costs imposed by the unauthorized disclosure and publication of users' content and information onto Plaintiffs and Class Members.

Facebook increased mitigation costs by failing to notify users that their content and information had been disclosed and to alert them at the earliest time possible so that users could take steps to protect their identities. In addition, Facebook increased mitigation costs by engaging in acts that furthered both the dissemination of user information and its aggregation, as well as by its failure to audit third parties who received user information to secure it. For example, Facebook failed to demand and enforce compliance with its policies by its own app developers, including that user data not be sold and that it be deleted if improperly obtained. In failing to mitigate, Facebook saved for itself costs it would have incurred, both out of pocket and loss of user engagement, and transferred those costs to Plaintiffs and Class Members.

420. Facebook's refusal to warn Plaintiffs, while transferring harm and risk to Plaintiffs, conferred benefits on itself. Warning Class Members would have chilled user engagement as well as potential new users from joining Facebook. It might have also involved scrutiny, which could have invited transaction costs, regulatory fines, shareholder concerns and a stock drop, which of course ultimately materialized. Facebook and CEO Zuckerberg were thus not only able to evade costs, but continue to accrue value. Moreover, by pushing off the reckoning day for Facebook's lapses, Facebook benefitted through the time value of money.

421. Facebook has also greatly benefitted by generating millions of additional dollars of revenue from the monetization of users' content and information. Facebook calculates and reports average revenue per user that is derived from Plaintiffs and Class Members' personal content. Advertisers, app developers and other third parties pay Facebook billions of dollars because of the access Facebook provides to Plaintiffs' and Class Members' content and information. Without the benefit of users' content and information, conferred on Facebook by Plaintiffs and Class Members, Facebook would not have had this access, and would not have been able to further monetize users' content and information. Had Facebook adhered to its agreement with Plaintiffs and Class Members by only accessing users' content and information to the extent they had given consent, or by disclosing to Plaintiffs and Class Members the true extent to which it allowed third parties to access content and information users intended to keep



private, Facebook would not have earned up to billions of dollars of additional revenue. As such, Facebook has effectively transferred the benefits denied to Plaintiffs and Class Members, as outlined above, to itself and to its third-party business partners in the form of additional revenues and denied Plaintiffs and Class Members the economic value, and resulting economic benefit, of users' content and information.

## **VI. PLAINTIFFS COULD NOT HAVE DISCOVERED THEIR CLAIMS UNTIL 2018.**

422. Facebook has consistently denied that it is careless about user content and information.

423. Christopher Wylie testified to the U.K. Parliament that in or around July 2014, Facebook's engineers may have assisted Cambridge Analytica with its harvesting of personal data of millions of Facebook users. Wylie testified that, according to Alexander Kogan, when the size of the transfer caused Facebook's platform to throttle the app—thereby effectively disabling the transfer of data—Cambridge Analytica reached out to Facebook for assistance.<sup>169</sup> Facebook “would have known from that moment about the project, because [Kogan would have] had a conversation with Facebook's engineers.”<sup>170</sup>

424. Even if the *Guardian's* December 2015 article regarding Cambridge Analytica's use of information about Facebook users had obliged Plaintiffs to conduct further investigation to determine whether they were among the Facebook users whose content and information was disclosed without permission, Plaintiffs would not have been able to uncover the facts underlying their claims.

425. That is because the relevant facts were in the possession of Facebook and Cambridge Analytica, and both refused to disclose them. In the wake of the December 2015 *Guardian* article, Facebook investigated Cambridge Analytica, but never publicly released the results of its investigation and until 2018 did not confirm that Plaintiffs' content and information

---

<sup>169</sup> House of Commons Digital, Culture, Media and Sport Comm., Oral Evidence: Fake News, HC 363, at Q1336 (Mar. 27, 2018), <http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/digital-culture-media-and-sport-committee/fake-news/oral/81022.pdf> (testimony of Christopher Wylie

<sup>170</sup> *Id.*

had been disclosed without their permission.

426. Indeed, Facebook actively concealed the facts.

427. In June 2016, it secured from Kogan and GSR a non-disclosure agreement about their collection of data, obliging them not to disclose the manner in which they obtained and used Plaintiffs' content and information. In exchange, Facebook waived and released any all claims against Kogan or GSR concerning the data.

428. Moreover, when Simon Milner, Facebook's Policy Director for the United Kingdom, the Middle East, and Africa, testified to the U.K. Parliament on February 8, 2018, he denied that Cambridge Analytica or any of its associated companies had "Facebook user data," and that, in any case, Facebook had "no insight on" how Cambridge Analytica may have gathered data from users on Facebook.<sup>171</sup>

429. Then, in a February 23, 2018 letter, Cambridge Analytica CEO Alexander Nix falsely told Parliament that "Cambridge Analytica does not gather such data,"<sup>172</sup> and Facebook did not correct or clarify Nix's false statement.

430. Four days later on February 27, Nix testified before Parliament. When asked whether any of Cambridge Analytica's data come from Facebook, Nix replied, "We do not work with Facebook data and we do not have Facebook data."<sup>173</sup> Nix also claimed that Cambridge Analytica "did not use any personality modelling or 'psychographics' in the election, and that it

---

<sup>171</sup> Digital, Culture, Media and Sport Committee (House of Commons), Examination of Witnesses Juniper Downs et al. at Q447-449, Feb. 8, 2018, <https://www.parliament.uk/business/committees/committees-a-z/commonsselect/digital-culture-media-and-sport-committee/inquiries/parliament-2017/fakenews-17-19/publications/>.

<sup>172</sup> Alexander Nix, *Letter from Alexander Nix, Chief Executive, Cambridge Analytica to Damian Collins, Chair of the Committee*, Feb. 23, 2018, <http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/digital-culture-media-and-sport-committee/fake-news/written/79053.pdf>.

<sup>173</sup> Digital, Culture, Media and Sport Committee (House of Commons), Examination of Witness Alexander Nix at Q3288, June 6, 2018, <http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/digital-culture-media-and-sport-committee/fake-news/oral/84838.html>.

has no access to Facebook likes.”<sup>174</sup> Once again, Facebook did not correct or clarify these false statements.

431. Only in March 2018, with the publication of articles by the *Guardian* and the *New York Times* did it become clear that Plaintiffs should inquire into whether they had been injured by Facebook’s misconduct. Thereafter, Facebook informed Facebook users that their content and information had been released to Cambridge Analytica.

## VII. CHOICE OF LAW

432. Facebook’s Terms of Service (formerly known as the “Statement of Rights and Responsibilities”) contain (and have always contained) a forum selection provision that mandates the resolution of any claim—arising either out of the Terms of Service or a person’s use of Facebook—exclusively in the U.S. District Court for the Northern District of California and provides that users submit to the personal jurisdiction of those courts to litigate those claims.

433. In addition, the Terms of Service contain (and have contained since at least April 26, 2011) a California choice-of-law provision.<sup>175</sup> The provision ensures that California law applies to “any claim that might arise between” a user and Facebook.<sup>176</sup>

434. This Court has consistently enforced the California choice of law provision.

## VIII. CLASS ACTION ALLEGATIONS

435. Plaintiffs incorporate by reference all the allegations of this complaint as though fully set forth herein.

436. Plaintiffs bring this action on behalf of themselves and all others similarly situated

---

<sup>174</sup> Alexander Nix, *Letter from Alexander Nix, Chief Executive, Cambridge Analytica to Damian Collins, Chair of the Committee*, Feb. 23, 2018,

<http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/digital-culture-media-and-sport-committee/fake-news/written/79053.pdf>.

<sup>175</sup> See, e.g., *Statement of Rights and Responsibilities*, Facebook (Apr. 26, 2011)

<http://www.facebook.com/legal/terms>

[<https://web.archive.org/web/20120529141325/http://www.facebook.com/legal/terms>] (“The laws of the State of California will govern this Statement, as well as any claim that might arise between you and us, without regard to conflict of law provisions”).

<sup>176</sup> *Id.*

pursuant to Rule 23(b)(2) and 23(b)(3) of the Federal Rules of Civil Procedure.

437. Plaintiffs seek to represent the following Classes:

A. **The Class**, which is defined as all Facebook users in the United States and in the United Kingdom whose content and information, generated when they were 18 years of age or older, was collected by Facebook and published and/or disclosed to third parties without their authorization or consent from January 1, 2007 to the present. The Class contains the following Subclasses:

i. **The Alabama Subclass**, which is defined as all members of the Class who resided in Alabama at the time the content and information they generated was collected by Facebook and published and/or disclosed to third parties without their authorization or consent.

ii. **The Colorado Subclass**, which is defined as all members of the Class who resided in Colorado at the time the content and information they generated was collected by Facebook and published and/or disclosed to third parties without their authorization or consent.

iii. **The Illinois Subclass**, which is defined as all members of the Class who resided in Illinois at the time the content and information they generated was collected by Facebook and published and/or disclosed to third parties without their authorization or consent.

iv. **The Iowa Subclass**, which is defined as all members of the Class who resided in Iowa at the time the content and information they generated was collected by Facebook and published and/or disclosed to third parties without their authorization or consent.

v. **The Kansas Subclass**, which is defined as all members of the Class who resided in Kansas at the time the content and information they generated was collected by Facebook and published and/or disclosed to third parties without their authorization or consent.

vi. **The Michigan Subclass**, which is defined as all members of the Class who resided in Michigan at the time that the content and information they generated was collected by Facebook and published and/or disclosed to third parties without their authorization or consent.

vii. **The New York Subclass**, which is defined as all members of the Class who resided in New York at the time that the content and information they generated was collected by Facebook and published and/or disclosed to third parties without their authorization or consent.

viii. **The Washington Subclass**, which is defined as all members of the Class who resided in Washington at the time that the content and information they generated was collected by Facebook and published and/or disclosed to third parties without their authorization or consent.

ix. **The West Virginia Subclass**, which is defined as all members of the Class who resided in West Virginia at the time that the content and information they generated was collected by Facebook and published and/or disclosed to third parties without their authorization or consent.

B. **The Minor Class**, which is defined as all Facebook users in the United States and in the United Kingdom whose content and information, generated when they were less than 18 years, was collected by Facebook and published and/or disclosed to third parties without their authorization or consent from January 1, 2007 to the present.

438. As used in this complaint, “Class Period” refers to the period January 1, 2007 to the present.

439. Excluded from the Classes are Defendants, their current employees, coconspirators, officers, directors, legal representatives, heirs, successors and wholly or partly owned subsidiaries or affiliated companies; the undersigned counsel for Plaintiffs and their employees; and the judge and court staff to whom this case is assigned. Plaintiffs reserve the right to amend the definitions of the Classes if discovery or further investigation reveals that the

Classes should be expanded or otherwise modified.

440. The Classes satisfy the prerequisites of Federal Rule of Civil Procedure 23(a) and the requirements of Rule 23(b)(3).

441. **Numerosity and Ascertainability:** Plaintiffs do not know the exact size of the Classes or the identities of the Class Members,<sup>177</sup> since such information is the exclusive control of Defendants. Nevertheless, the Class encompasses millions of individuals, and the Minor Class encompasses—at the least—thousands of individuals, dispersed throughout the United States and the United Kingdom. Each of the Subclasses also contains at least thousands, and almost certainly more, individuals. The number of members in each of the Classes is so numerous that joinder of all members in any of the Classes is impracticable. The names, addresses, and phone numbers of Class Members are identifiable through documents maintained by Defendants.

442. **Commonality and Predominance:** The action involves common questions of law and fact, which predominate over any question solely affecting individual Class Members.

These common questions include:

- i. Whether Facebook gave Plaintiffs and Class Members effective notice of its program to collect their content and information;
- ii. Whether Defendants obtained authorization or consent from Plaintiffs and class members to collect their content and information;
- iii. Whether Defendants improperly collected Plaintiffs' and Class Members' content and information;
- iv. Whether Facebook represented that Plaintiffs' and Class Members' content and information would be protected from disclosure absent their consent;
- v. Whether Facebook owes any duty to Plaintiffs and Class Members with respect to maintaining, securing, or deleting their content and information;
- vi. To what degree Facebook has the right to use content and information pertaining to Plaintiffs and Class Members;
- vii. Whether Facebook owed a legal duty to Plaintiffs and the Classes to exercise due care in collecting, storing, safeguarding, and/or obtaining their content and information;

---

<sup>177</sup> Here and elsewhere in the complaint, the term “Class Members” refers collectively to Members of all Classes.

- viii. Whether Facebook breached a legal duty to Plaintiffs and the Classes to exercise due care in collecting, storing, safeguarding, and/or obtaining their content and information;
- ix. Whether the egregious breach of privacy and trust alleged in the Complaint was foreseeable by Facebook;
- x. Whether Facebook intentionally exposed Plaintiffs' and Class Members' content and information to Cambridge Analytica;
- xi. Whether Defendants violated the Stored Communications Act;
- xii. Whether Defendants violated Plaintiffs' and Class Members' privacy rights;
- xiii. Whether Facebook's conduct was an unlawful or unfair business practice under Cal. Bus. & Prof. Code §§ 17200 *et seq.* (West 2018);
- xiv. Whether Facebook is a "video tape service provider" under 18 U.S.C. § 2710.
- xv. Whether Facebook is a provider of electronic communication service to the public pursuant to 18 U.S.C. §§ 2702(a)(1) and 2510(15).
- xvi. Whether Facebook maintains a facility through which an electronic communication service is provided, pursuant to 18 U.S.C. § 2701(a).
- xvii. Whether Facebook is a provider of a remote computing service to the public, pursuant to 18 U.S.C. §§ 2702(a)(2) and 2711(2).
- xviii. Whether "Facebook content," a term defined below, constitutes electronic communications under 18 U.S.C. § 2510(12).
- xix. Whether Plaintiffs and the Class are "users" or "subscribers" of Facebook's remote computing service, as the term "user" is defined and/or used in 18 U.S.C. § 2510(5) and (13)
- xx. Whether Plaintiffs and the members of the Classes are "aggrieved person[s]" as that term is defined in 18 U.S.C. § 2510(11).
- xxi. Whether Plaintiffs' and the Class Members' use of Facebook's messaging systems and transfers of content and information to Facebook constitute electronic communications, pursuant to 18 U.S.C. § 2501(12).
- xxii. Whether Plaintiffs' and Class Members' electronic communications were in electronic storage, pursuant to 18 U.S.C. § 2501(17).
- xxiii. Whether Facebook knowingly divulged the contents of Plaintiffs and the Class Members' electronic communications while they were in electronic storage to unauthorized parties in violation of 18 U.S.C. § 2702(a)(1).
- xxiv. Whether Facebook knowingly divulged the contents of Plaintiffs' and Class Members' electronic communications that were carried or maintained on Facebook's remote computing service to unauthorized parties in violation of 18 U.S.C. § 2702(a)(2).
- xxv. Whether Plaintiffs and the members of the Classes have suffered an injury as a result of Facebook's violations of the Stored Communications Act.



- xxvi. Whether Facebook profited from its acts that violate the Stored Communications Act.
- xxvii. Whether Facebook’s violation of the Stored Communications Act committed willfully and intentionally.
- xxviii. Whether Facebook is a “video tape service provider” as that term is defined in 18 U.S.C. § 2710.
- xxix. Whether Plaintiffs and members of the Classes are “consumers” as that term is defined in 18 U.S.C. § 2710.
- xxx. Whether Plaintiffs’ and the other Class Members’ data that Facebook possessed contained “personally identifiable information” as that term is defined in 18 U.S.C. § 2710.
- xxxi. Whether Facebook knowingly allowed third parties access to Plaintiffs’ and Class Members’ personally identifiable information in violation of the Video Privacy Protection Act.
- xxxii. Whether Plaintiffs and the other Class members are “aggrieved person[s]” as that term is defined by 18 U.S.C. § 2710.
- xxxiii. Whether Facebook suppressed facts which it was bound to disclose to Plaintiffs and members of the Classes about the privacy of their user content and information.
- xxxiv. Whether Facebook gave information of facts that were likely to mislead Plaintiffs and members of the Classes about the privacy of their user content and information.
- xxxv. Whether Facebook failed to disclose known risks that third-party app developers would sell or disperse Plaintiffs’ and Members of the Classes’ user content and information without their consent.
- xxxvi. Whether Facebook violated the terms of an October 2012 FTC settlement by continuing to allow app developers access to Plaintiffs and Class Member’s user content and information without their consent.
- xxxvii. Whether Facebook failed to audit whether and how Plaintiffs’ and the Class Members’ user content and information was provided to third parties.
- xxxviii. Whether Facebook failed to disclose to Plaintiffs and the members of the Classes the risks that each faced from the disclosure of their user content and information.
- xxxix. Whether Facebook failed to inform Plaintiffs and the members of the Classes that their user content and information was insecure once it was shared with app developers or other third parties.
- xl. Whether Facebook knew that Plaintiffs’ and Class Members’ user content and information was not secure.
- xli. Whether Facebook ignored warnings that audits were necessary to secure Plaintiffs’ and Class Members’ user content and information.

- xlii. Whether Facebook intentionally failed to secure Plaintiffs' and Class Members' information and content.
- xliii. Whether Facebook had a duty to inform Plaintiffs and members of the Classes that Facebook had become aware that it had failed to secure Plaintiffs' and Class Members' user content and information.
- xliv. Whether Defendants intentionally concealed that Plaintiffs' and Class Members' user content and information was insecure.
- xlvi. Whether failed to disclose to Plaintiffs and members of the Classes that it had not secured their user content and information.
- xlvi. Whether Defendants failed to disclose to Plaintiffs and the Class of the risks that each faced from Facebook's failure to secure user content and information.
- xlvi. Whether Facebook intended to deceive Plaintiffs and the members of the Classes about the security of their user content and information.
- xlvi. Whether Plaintiffs and the members of the Classes were damaged because as a result of Defendants' deceit.
- xlix. Whether Facebook misled Plaintiffs and the members of the Classes to believe that Facebook was protecting users' privacy.
  - i. Whether Facebook failed to disclose to or deceived Plaintiffs and the members of the Classes that Facebook was sharing their users content and information with third parties.
  - ii. Whether Facebook failed to disclose that, notwithstanding privacy settings that purported to provide Plaintiffs and members of the Classes with control over their user content and information, Facebook allowed third-parties to harvest and store Plaintiffs' and the Class Members' personal information.
  - iii. Whether Facebook had a duty to provide accurate information to Plaintiffs and members of the Classes about how their user content and information was disclosed to third parties.
  - iv. Whether Facebook encouraged Plaintiffs and members of the Classes to share content and information by assuring them that Facebook would respect their choices concerning privacy.
  - v. Whether Facebook intentionally concealed how it disclosed Plaintiffs' and Class Members' user content and information and whether it did so to create a false sense of security and privacy for Plaintiffs and Class Members.
  - vi. Whether Facebook intentionally concealed how it disclosed Plaintiffs' and Class Members' user content and information in order to increase its revenues.
  - vii. Whether Plaintiffs and members of the Classes were damaged because their user content and information were disclosed to third party device makers and other business partners without their consent.

- lvii. Whether Facebook failed to disclose to Plaintiffs and members of the Classes how their user content and information was being collected, shared and aggregated to develop digital profiles or dossiers of each user.
- lviii. Whether Defendants had a duty to disclose the full extent to which it allowed Plaintiffs and members of the Classes to be targeted by advertisers and marketers.
- lix. Whether Facebook knew that advertisers and marketers were targeting Plaintiffs and members of the Classes with messages based upon Facebook-derived content and information.
- lx. Whether Facebook failed to disclose to Plaintiffs and members of the Classes that advertisers were combining data from data brokers with Facebook-derived content and information to target them with advertisements and psychographic marketing, as well as building digital dossiers of users.
- lxi. Whether Facebook intended to deceive Plaintiffs and members of the Classes about their vulnerability to targeted advertisements.
- lxii. Whether Facebook has been unjustly enriched by virtue of its deceit concerning user content and information disclosure and aggregation for advertisers.
- lxiii. Whether Facebook must disgorge its profits made from the use of Plaintiffs' and Class Members' content and information.
- lxiv. Whether Plaintiffs and members of the Classes had a reasonable expectation that their user content and information they entrusted to Facebook would be protected and secured against access by unauthorized parties and would not be disclosed to or obtained by unauthorized parties, or disclosed or obtained for any improper purpose.
- lxv. Whether Facebook intentionally intruded upon the private affairs and concerns of Plaintiffs and members of the Classes.
- lxvi. Whether Facebook intrusions upon the private affairs and concerns of Plaintiffs and members of the Classes were substantial, and would be highly offensive to a reasonable person.
- lxvii. Whether Plaintiffs and members of the Classes did not consent to Facebook's intrusions upon their private affairs and concerns.
- lxviii. Whether Plaintiffs and members of the Classes suffered actual and concrete injury as a result of Facebook's intrusions upon Plaintiffs' and Class Members' private affairs and concerns.
- lxix. Whether Plaintiffs and members of the Classes are entitled to relief for their injuries that resulted from Facebook's intrusion upon Plaintiffs' and Class Members' private affairs and concerns.
- lxx. Whether Facebook published private content and information of Plaintiffs and members of the Classes to unauthorized parties and failed to take reasonable steps to prevent further dissemination of this content and information.

- lxxi. Whether Facebook’s publication of Plaintiffs’ and Class Members’ user content and information would be highly offensive to a reasonable person.
- lxxii. Whether Plaintiffs’ and Class Members’ content and information was private and not of legitimate public concern or substantially connected to a matter of legitimate public concern.
- lxxiii. Whether Plaintiffs and members of the Classes suffered injury as a result of Facebook’s publication of Plaintiffs’ and Class Members’ content and information.
- lxxiv. Whether Facebook and Plaintiffs and members of the Classes mutually assented to, and therefore were bound by the version of Facebook’s Statement of Rights and Responsibilities or later, the Terms of Service, (collectively, the “Contracts”) that was operative at the time each of the Plaintiff or a member of the Classes joined Facebook.
- lxxv. Whether the Contracts required Facebook to protect the content and information of its users, including Plaintiffs and members of the Classes.
- lxxvi. Whether the Contracts failed to form or obtain consent to share Plaintiffs’ and Class Members’ user content and information with advertisers and other third parties and/or failed to disclose that such information would be shared if users’ friends entered into an agreement which permitted third parties to collect their friends’ information.
- lxxvii. Whether Facebook made it unreasonably difficult for Plaintiffs and members of the Classes to access the provisions of the Privacy and Data Use Policies, and particularly the provision of the Privacy and Data Use Policies disclosing friend-of-user sharing.
- lxxviii. Whether Facebook made it unreasonably difficult for Plaintiffs and members of the Classes to understand which privacy settings governed how third-party applications and advertisers could access users’ content and information via friend-of user sharing.
- lxxix. Whether Facebook failed to adequately explain to Plaintiffs and members of the Classes that a user’s “Privacy settings” were ineffective in controlling whether users’ content and information was shared via friend-of-user sharing.
- lxxx. Whether, contrary to the Contracts, Facebook knowingly allowed Doe Defendants to sell the personally identifiable information regarding Plaintiffs and members of the Classes that they had collected via applications that used the Facebook platform.
- lxxxi. Whether Plaintiffs’ and Class Members’ content and information has value.
- lxxxii. Whether Facebook breached the Contracts.
- lxxxiii. Whether Facebook owed a duty to Plaintiffs and members of the Classes to exercise reasonable care in the obtaining, using, and protecting of their content and information, arising from the sensitivity of their content and information and the expectation that their content and information was not going to be shared with third parties without their consent.

- lxxxiv. Whether Facebook owed a duty to timely disclose to Plaintiffs and members of the Classes that Facebook had allowed their content and information to be accessed by third parties.
- lxxxv. Whether Facebook knew that the content and information of Plaintiffs and members of the Classes had value.
- lxxxvi. Whether Facebook failed to take reasonable steps to prevent harm to Plaintiffs from known threats to the security to Plaintiffs' and Class Members' user content and information.
- lxxxvii. Whether Facebook breached the duties of care it owed to Plaintiffs and members of the Classes.
- lxxxviii. Whether Plaintiffs and members of the Classes were foreseeable victims of Facebook's breach of its duties.
- lxxxix. Whether, as a result of Facebook's negligent failure to safeguard Plaintiffs' and Class Members' content and information, Plaintiffs and members of the Classes members have suffered injuries.
- xc. Whether the injuries to Plaintiff and members of the Classes were proximate, reasonably foreseeable results of Facebook's breaches of its duties of care.
- xc. Whether it is reasonable for Plaintiffs and members of the Classes to obtain identify protection and/or credit monitoring services in light of the Facebook's breath of its duties of care.
- xcii. Whether Public policy would void any purported waiver of liability to which Facebook may claim.
- xciii. Whether Facebook's conduct constitutes gross negligence.
- xciv. Whether Plaintiffs and members of the Classes have a privacy right to their user content and information under Art. I, Sec. 1 of the California Constitution.
- xcv. Whether Facebook violated Plaintiffs' and Class Members' constitutionally-protected right to privacy.
- xcvi. Whether Facebook violated the common law prohibition on the use of a person's name or likeness to its own advantage.
- xcvii. Whether Facebook failed to obtain consent from Plaintiffs and Members of the Classes to use their likenesses.
- xcviii. Whether Plaintiffs and members of the Classes received no compensation in return for Facebook's use of their likenesses.
- xcix. Whether Plaintiffs and members of the Classes were harmed by Facebook's improper use of their likenesses.
- c. Whether Facebook knowingly obtained benefits from Plaintiffs and members of the Classes under circumstances such that it would be inequitable and unjust for Facebook to retain them.
- ci. Whether Facebook is a "person" as defined by Ala. Code § 8-19-3(5).

- cii. Whether Facebook's products and services are "goods" and "services" as defined by Ala. Code § 8-19-3(3), (7).
- ciii. Whether Facebook advertised, offered, or sold goods or services in Alabama and engaged in trade or commerce directly or indirectly affecting the people of Alabama as defined by Ala. Code § 8-19-3(8).
- civ. Whether Facebook engaged in unconscionable, false, misleading or deceptive practices in connection with its business, commerce and trade practices in violation of Ala. Code § 8-19-5(27).
- cv. Whether Facebook acted intentionally, knowingly, and maliciously to violate Alabama's Deceptive Trade Practices Act, and recklessly disregarded the Alabama Plaintiff's and the Alabama Subclass members' rights.
- cvi. Whether Facebook is a "person" as defined by Colo. Rev. Stat. Ann. § 6-1-102(6).
- cvii. Whether the Colorado Plaintiff and Colorado Subclass members, as well as the general public, are actual or potential consumers of the services offered by Facebook to actual consumers.
- cvi. Whether Facebook engaged in deceptive trade practices in the course of its business, in violation of Colo. Rev. Stat. Ann. § 6-1-105(1)(u).
- cix. Whether Facebook engaged in deceptive trade practices in the course of its business, in violation of Colo. Rev. Stat. Ann. § 6-1-105(3) by engaging unfair trade practices actionable at common law or under other statutes of Colorado.
- cx. Whether Facebook intended to mislead the Colorado Plaintiff and the Colorado Subclass members and induce them to rely on its misrepresentations and omissions.
- cx. Whether Facebook acted fraudulently, willfully, knowingly, or intentionally to violate Colorado's Consumer Protection Act, and with recklessly disregarded the Colorado Plaintiff's and the Colorado Subclass members' rights.
- cxii. Whether Facebook is a "person" as defined by 815 Ill. Comp. Stat. Ann. § 505/1(c).
- cxiii. Whether the Illinois Plaintiffs and the Illinois Subclass members are "consumer[s]" as defined by 815 Ill. Comp. Stat. Ann. § 505/1(e).
- cxiv. Whether Facebook's conduct as described herein was in the conduct of "trade" or "commerce" as defined by 815 Ill. Comp. Stat. Ann. § 505/1(f).
- cxv. Whether Facebook's deceptive, unfair, and unlawful trade acts or practices, in violation of 815 Ill. Comp. Stat. Ann. § 505/2.
- cxvi. Whether Facebook acted intentionally, knowingly, and maliciously to violate Illinois's Consumer Fraud and Deceptive Business Practices Act, and recklessly disregarded the Illinois Plaintiffs and the Illinois Subclass members' rights.
- cxvii. Whether Facebook is a "person" as defined by Iowa Code Ann. § 714H.2(7).



- cxviii. Whether the Iowa Plaintiff and the Iowa Subclass members are “consumer[s]” as defined by Iowa Code § 714H.2(3).
- cxix. Whether Facebook’s conduct described herein related to or was in connection with the “sale” or “advertisement” of “merchandise” as defined by Iowa Code Ann. § 714H.2(2), (6), (8).
- cxx. Whether Facebook engaged in unfair, deceptive, and unconscionable trade practices, in violation of the Iowa Private Right of Action for Consumer Frauds Act, as described throughout and herein.
- cxxi. Whether Facebook acted intentionally, knowingly, and maliciously to violate Iowa’s Private Right of Action for Consumer Frauds Act, and recklessly disregarded the Iowa Plaintiff and the Iowa Subclass members’ rights.
- cxxii. Whether the Kansas Plaintiff and the Kansas Subclass members are “consumer[s]” as defined by Kan. Stat. Ann. § 50-624(b).
- cxxiii. Whether the acts and practices described herein are “consumer transaction[s],” as defined by Kan. Stat. Ann. § 50-624(c).
- cxxiv. Whether Facebook is a “supplier” as defined by Kan. Stat. Ann. § 50-624(l).
- cxxv. Whether Facebook advertised, offered, or sold goods or services in Kansas and engaged in trade or commerce directly or indirectly affecting the people of Kansas.
- cxxvi. Whether the Kansas Plaintiff and the Kansas Subclass members had unequal bargaining power with respect to their use of Facebook’s services because of Facebook’s omissions and misrepresentations.
- cxxvii. Whether Facebook acted intentionally, knowingly, and maliciously to violate Kansas’s Consumer Protection Act, and recklessly disregarded the Kansas Plaintiff and the Kansas Subclass members’ rights.
- cxxviii. Whether Facebook, the Michigan Plaintiff, and Michigan Subclass members are “person[s]” as defined by Mich. Comp. Laws Ann. § 445.902(1)(d).
- cxxix. Whether Facebook advertised, offered, or sold goods or services in Michigan and engaged in trade or commerce directly or indirectly affecting the people of Michigan, as defined by Mich. Comp. Laws Ann. § 445.902(1)(g).
- xxxx. Whether Facebook engaged in unfair, unconscionable, and deceptive practices in the conduct of trade and commerce, in violation of Mich. Comp. Laws Ann. § 445.903(1).
- xxxxi. Whether Facebook engaged in deceptive acts or practices in the conduct of its business, trade, and commerce or furnishing of goods or services, in violation of N.Y. Gen. Bus. Law § 349, as described herein.
- xxxxii. Whether Facebook acted intentionally, knowingly, and maliciously to violate New York’s General Business Law, and recklessly disregarded the New York Plaintiff’s and the New York Subclass members’ rights.
- xxxxiii. Whether Facebook is a “[p]erson,” as defined by Wash. Rev. Code Ann. § 19.86.010(1).



- cxxxiv. Whether Facebook advertised, offered, or sold goods or services in Washington and engaged in trade or commerce directly or indirectly affecting the people of Washington, as defined by Wash. Rev. Code Ann. § 19.86.010(2).
- cxxxv. Whether Facebook engaged in unfair or deceptive acts or practices in the conduct of trade or commerce, in violation of Wash. Rev. Code Ann. § 19.86.020, as described herein.
- cxxxvi. Whether Facebook acted intentionally, knowingly, and maliciously to violate Washington’s Consumer Protection Act, and recklessly disregarded the Washington Plaintiff’s and Washington Subclass members’ rights.
- cxxxvii. Whether the West Virginia Plaintiffs and West Virginia Subclass members are “[c]onsumer[s],” as defined by W. Va. Code Ann. § 46A-6-102(2).
- cxxxviii. Whether Facebook engaged in “consumer transaction[s],” as defined by W. Va. Code Ann. § 46A-6-102(2).
- cxxxix. Whether Facebook advertised, offered, or sold goods or services in West Virginia and engaged in trade or commerce directly or indirectly affecting the people of West Virginia, as defined by W. Va. Code Ann. § 46A-6-102(6).
- cxl. Whether Facebook’s unfair and deceptive acts and practices violated W. Va. Code Ann. § 46A-6-102(7).
- cxli. Whether Facebook’s unfair and deceptive acts and practices were unreasonable when weighed against the need to develop or preserve business, and were injurious to the public interest, under W. Va. Code Ann. § 46A-6-101.
- cxlii. Whether Facebook’s acts and practices were “[u]nfair” under W. Va. Code Ann. § 46A-6-104 because they caused or were likely to cause substantial injury to consumers which was not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.
- cxliii. Whether Facebook’s acts and practices were “deceptive” under W. Va. Code Ann. § 46A-6-104.
- cxliv. Whether Facebook’s omissions were legally presumed to be equivalent to active misrepresentations because Facebook intentionally prevented the West Virginia Plaintiff and the West Virginia Subclass members from discovering the truth regarding Facebook’s use, sale, disclosure and abuse of private user data.
- cxlv. Whether Facebook acted intentionally, knowingly, and maliciously to violate West Virginia’s Consumer Credit and Protection Act, and recklessly disregarded the West Virginia Plaintiff’s and the West Virginia Subclass members’ rights.
- cxlvi. Whether Facebook’s deceptive trade practices significantly impact the public.
- cxlvii. Whether Facebook’s representations and omissions were material because they were likely to deceive reasonable consumers.

- cxlviii. Whether Facebook intended that the Alabama, Colorado, Illinois, Iowa, Kansas, Michigan, New York, Washington, and West Virginia Plaintiffs and the various Subclass members would rely on its misrepresentations, omissions, and other unlawful conduct.
- cxlix. Whether, as a direct and proximate result of Facebook's unfair and deceptive acts and practices, Alabama, Colorado, Illinois, Iowa, Kansas, Michigan, New York, Washington, and West Virginia Plaintiffs and the various Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages.
- cl. Whether the Alabama, Colorado, Illinois, Iowa, Kansas, Michigan, New York, Washington, and West Virginia Plaintiffs and the various Subclass members have suffered injuries in fact and lost money or property due to Facebook's business acts or practices.
- cli. Whether Plaintiffs and the Classes are entitled to equitable relief, including, but not limited to, injunctive relief, restitution, and disgorgement; and
- clii. Whether Plaintiffs and the Classes are entitled to actual, statutory, or other forms of damages, and other monetary relief.

443. Defendants engaged in a common course of conduct giving rise to the legal rights sought to be enforced by this action and similar or identical questions of statutory and common law, as well as similar or identical injuries, are involved. Individual questions, if any, pale in comparison to the numerous common questions that predominate in this action.

444. **Typicality:** Plaintiffs' claims are typical of the other Class Members' claims because all Class Members were comparably injured through Defendants' substantially uniform misconduct as described above. The Plaintiffs representing the Classes are advancing the same claims and legal theories on behalf of themselves and all other members of the Classes that they represent, and there are no defenses that are unique to Plaintiffs. The claims of Plaintiffs and Class Members arise from the same operative facts and are based on the same legal theories.

445. **Adequacy:** Plaintiffs are adequate Class representatives because their interests do not conflict with the interests of the other members of the Classes they seek to represent; Plaintiffs have retained counsel competent and experienced in complex class action litigation, and Plaintiffs intend to prosecute this action vigorously. The Classes' interest will be fairly and adequately protected by Plaintiffs and their counsel.

446. **Superiority:** A class action is superior to any other available means for the fair

and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages and other detriment suffered by Plaintiffs and the other class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendants, so it would be virtually impossible for the members of the Classes to individually seek redress for Defendants' wrongful conduct. Even if class members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties, and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

447. Class certification under Rule 23(b)(2) is also warranted for purposes of injunctive and declaratory relief because Defendants have acted or refused to act on grounds generally applicable to the Classes, so that final injunctive and declaratory relief are appropriate with respect to each Class as a whole.

## IX. CAUSES OF ACTION

448. Pursuant to 28 U.S.C. § 1407(a), this complaint consolidates claims of all plaintiffs in this multidistrict litigation and proposes priority briefing for certain claims. In the event that Defendants seek to challenge claims asserted herein via motion pursuant to FRCP 12, Plaintiffs propose that twelve of the claims asserted herein be briefed in priority. Those claims are set forth herein as Part A.

### A. Prioritized Claims

**Claim I. Violation of the Stored Communications Act ("SCA"),  
18 U.S.C. §§ 2701 *et seq.*  
(Against Prioritized Defendant Facebook and Doe Defendants, and Against Non-Prioritized  
Defendants Zuckerberg, Kogan)  
On Behalf of All Plaintiffs and All Classes**

449. Plaintiffs incorporate by reference all allegations of this complaint as though fully set forth herein.

450. The Stored Communications Act (“SCA”) allows a private right of action against anyone who “(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system.” *See* 18 U.S.C. § 2701(a); *see also* 18 U.S.C. § 2707(a) (cause of action).

451. The Electronic Communications Privacy Act, 18 U.S.C. §§ 2510, *et seq.*, defines an “electronic communication” as “any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce.” 18 U.S.C. § 2510(12). The SCA incorporates this definition of “electronic communication.”

452. To create the information transferred to Facebook such as all posts, private messages, and similar communication (collectively “Facebook content”), Facebook users transmit writing, images, or other data via the Internet from their computers or mobile devices to Facebook’s servers. This Facebook content, therefore, constitutes electronic communications for purposes of the SCA.

453. The SCA distinguishes between two types of electronic storage. The first is defined as “any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof.” 18 U.S.C. § 2510(17)(A). The second type is defined as “any storage of such communication by an electronic communication for purposes of backup protection of such communication.” 18 U.S.C. § 2510(17)(B). Because Facebook saves and archives Facebook content indefinitely, Facebook content is stored in electronic storage for purposes of the SCA.

454. Facebook allows users to select privacy settings for their Facebook content. Access can be limited to a user’s Facebook friends, to particular groups or individuals, or to just the particular Facebook user. When users make Facebook content inaccessible to the general public, the information is considered private for purposes of the SCA.

455. As set forth herein, Plaintiffs did not authorize Defendants to share their content and information with Facebook's third party "partners" such as device makers or app developers in violation of users' personal privacy settings.

456. Plaintiffs are subscribers or customers of Facebook's remote computing service, pursuant to 18 U.S.C. § 2702(a)(2). By virtue of Facebook's conduct in providing the ability to send or receive wire or electronic communications, Facebook is an electronic communication service within the meaning of the SCA. Plaintiffs and Class Members are users of Facebook's electronic communication service, pursuant to 18 U.S.C. § 2510(13).

457. Plaintiffs are subscribers and persons aggrieved by violations of the SCA, pursuant to 18 U.S.C. §§ 2707(a) and 2510(11).

458. By virtue of Defendants' conduct in providing computer storage and processing services by means of an electronic communications system, Facebook is a remote computer service within the meaning of the SCA.

459. Facebook is a provider of an electronic communication service to the public, pursuant to 18 U.S.C. §§ 2702(a)(1) and 2510(15).

460. Facebook maintains a facility through which an electronic communication service is provided, pursuant to 18 U.S.C. § 2701(a).

461. Facebook is a provider of a remote computing service to the public, pursuant to 18 U.S.C. §§ 2702(a)(2) and 2711(2).

462. Facebook and Doe Defendants are persons within the meaning of the SCA, pursuant to 18 U.S.C. § 2510(6).

463. Facebook and Doe Defendants are persons or entities within the meaning of the SCA, pursuant to 18 U.S.C. § 2707(a).

464. Plaintiffs' and Class Members' use of Facebook's messaging systems and transfers of content and information to Facebook constitute electronic communications, pursuant to 18 U.S.C. § 2501(12).

465. Plaintiffs' and Class Members' electronic communications were in electronic storage, pursuant to 18 U.S.C. § 2501(17).

466. Defendants violated the SCA by intentionally accessing without authorization or exceeding an authorization to access Facebook's facility through which an electronic communication service is provided, thereby obtaining access to Plaintiffs' and Class Members' electronic communications while they were in electronic storage, pursuant to 18 U.S.C. § 2701(a).

467. Facebook violated the SCA by knowingly divulging the contents, including content and information, of Plaintiffs' and Class Members' electronic communications while they were in electronic storage to unauthorized parties, including but not limited to Cambridge Analytica and Doe Defendants, pursuant to 18 U.S.C. § 2702(a)(1).

468. Facebook violated the SCA by knowingly divulging the contents, including content and information, of Plaintiffs' and Class Members' electronic communications that were carried or maintained on Facebook's remote computing service to unauthorized parties, including but not limited to Cambridge Analytica and Doe Defendants, pursuant to 18 U.S.C. § 2702(a)(2).

469. As a result of Defendants' violations of the SCA, Plaintiffs and Class Members have suffered injury, including but not limited to the invasion of Plaintiffs' and Class Members' privacy rights.

470. Defendants profited through their violations of the SCA, and Plaintiffs suffered actual damages, as detailed herein, as a result of these violations, pursuant to 18 U.S.C. § 2707(c).

471. Plaintiffs and Class Members are entitled to actual damages, disgorgement of profits made by Defendants as a result of their violations of the SCA, and statutory damages, in an amount not less than \$1,000 per Plaintiff or Class Member,

472. Plaintiffs are also entitled to preliminary and other equitable or declaratory relief as may be appropriate, as well as reasonable attorneys' fees and litigation costs, pursuant to 18 U.S.C. § 2707(b).

473. Defendants' violations of the SCA were committed willfully and intentionally, and therefore Plaintiffs and Class Members also seek punitive damages pursuant to 18 U.S.C. § 2707(c).

**Claim II. Violation of Video Privacy Protection Act, 18 U.S.C. § 2710  
(Against Prioritized Defendant Facebook and Doe Defendants, and Against Non-Prioritized  
Defendants Kogan, Zuckerberg)  
On Behalf of All Plaintiffs and All Classes**

474. Plaintiffs incorporate by reference all allegations of this complaint as though fully set forth herein.

475. Facebook is a "video tape service provider" under 18 U.S.C. § 2710 because it is a person "engaged in the business, in or affecting interstate or foreign commerce, of rental, sale, or delivery of prerecorded video cassette tapes or similar audio-visual materials." 18 U.S.C. § 2710(a)(4). Facebook regularly displays a variety of video content to its users.

476. Plaintiffs and the other Class members are "consumers" under 18 U.S.C. § 2710 because they are subscribers of goods or services from Facebook, a video tape service provider. 18 U.S.C. § 2710(a)(1).

477. The Facebook data of Plaintiffs and the other Class members contained "personally identifiable information" under 18 U.S.C. § 2710 because the information identified Plaintiffs and the other Class members as having requested or obtained specific video materials or services from Facebook, a video tape service provider, and included other information ordinarily used to identify individuals, such as Facebook user IDs, names, addresses and similar information.

478. GSR obtained access to users' and users' friends likes. As alleged above, this information included specific video information about these users. GSR sold this information to Cambridge Analytica. Thus, Defendants knowingly allowed GSR and Cambridge Analytica to access and share the specific video preferences of its users through this "likes" information without their authorization.

479. Facebook knowingly allowed app developers, including GSR, access to all of the posts in a user's timeline. This information included videos uploaded by the user as well as



videos or video hyperlinks shared with a user by the user's friends. It also included posts by that user, or posts shared with that user, about videos.

480. Facebook allowed its third-party partners, including but not limited to device makers, mobile carriers, software makers, security firms and chip designers, to access Plaintiffs' content and information without consent and in violation of Plaintiffs' personal privacy settings. Facebook knowingly disclosed Plaintiffs' and the other Class members' content and information to third parties, including GSR and other app developers, without the informed, written consent of Plaintiffs and the other Class members.

481. Plaintiffs and the other Class members are "aggrieved person[s]" under the VPPA by Facebook's disclosure of their personally identifiable information under 18 U.S.C. § 2710, as alleged herein. Therefore, Plaintiffs and the other Class members may bring an action under § 2710(c) against Facebook.

482. Plaintiffs and the other Class members may be awarded actual damages, but not less than liquidated damages in an amount of \$2,500 per Plaintiff, punitive damages, attorneys' fees and costs, and such other preliminary and equitable relief as the court determines to be appropriate.

**Claim III. Deceit by Concealment or Omission**  
**Cal. Civ. Code §§ 1709 & 1710**  
**(Against Prioritized Defendant Facebook and Doe Defendants)**  
**On Behalf of All Plaintiffs and All Classes**

483. Plaintiffs incorporate by reference all allegations of this complaint as though fully set forth herein.

484. Under California law, a plaintiff may assert a claim for deceit by concealment based on "[t]he suppression of a fact, by one who is bound to disclose it, or who gives information of other facts which are likely to mislead for want of communication of that fact." Cal. Civ. Code § 1710(3).

485. These following actions are "deceit" under Cal. Civil Code § 1710 because Facebook suppressed facts that they were duty-bound to disclose, especially given Facebook's assertions about protecting the privacy of Plaintiffs and Class Members. Facebook has

committed deceit by concealment in three distinct ways.

486. **First**, Facebook did not disclose known risks that third party app developers would sell or disperse user content and information.

487. Facebook received multiple warnings that Plaintiffs' and the Class Members' content and information was at risk.

- (1) In 2012, Sandy Parakilas, former Facebook operations manager, warned Facebook's executives about the risks of app developers gaining access to users' personal information without their consent on Facebook's platform. Yet, Facebook ignored Parakilas's warnings.
- (2) In October 2012, Facebook reached a settlement with the FTC agreeing to clearly and prominently disclose its sharing of information with third parties; yet, Facebook continued to let app developers access users' information without their consent.
- (3) As late as 2017, Alex Stamos, Facebook's former Chief of Security, warned Facebook executives about security risks on the platform. In an internal meeting held in 2017, Stamos warned of "intentional decisions to give access to data and systems to engineers to make them 'move fast' but that creates other issues for us."
- (4) In 2017, Stamos states that he provided a written report concerning the circumstances leading to Cambridge Analytica obtaining users' personal information. Facebook edited and published a whitewashed version of this report concealing any wrongdoing.

488. Facebook did not audit what happened to content and information that was provided to third parties because it knew it would find abuse. Facebook did not disclose to Plaintiffs or Class Members the risks that they faced from these warnings, and did not inform Plaintiffs or Class Members that their content and information was insecure once it was shared with app developers or other third parties.

489. Facebook knew that Plaintiffs' and Class Members' content and information was

not secure. Facebook ignored the warnings above that audits were necessary to secure Plaintiffs' and Class Members' content and information because Defendants did not know what third parties were doing with it after it left Facebook's servers.

490. Defendants intentionally failed to secure Plaintiffs' and Class Members' information and content because they wanted to encourage third-party app developers and other business partners to exploit that information and content. Defendants knew that appropriate security measures—such as audits—would discourage third-parties. Defendants did not engage in such audits or conduct other reasonable efforts to protect Plaintiffs' and Class Members' content and information.

491. Defendants had a duty to inform Plaintiffs and Class Members that Defendants had become aware that they had failed to secure their content and information. Facebook knew in 2015 that it had failed to secure Plaintiffs' and Class Members' content and information, including by making it available to Facebook's business partners, including but not limited to device makers, mobile carriers, software makers, security firms and chip designers.

492. Defendants intentionally concealed that Plaintiffs' and Class Members' information and content was insecure because they wanted Plaintiffs and Class Members to continue to generate content for their business partners. Defendants failed to disclose the risks Plaintiffs and Class Members faced with the intention to deceive them about the security of their content and information.

493. Defendants failed to disclose to Plaintiffs and Class Members that it had failed to secure content and information for dozens of other third-party apps, even after it became aware of abuse in 2015 with the Cambridge Analytica Scandal, and conducted no investigation of the extent to which it had failed to do so until March of 2018.

494. Had Plaintiffs and Class Members been aware that Defendants had failed to implement adequate security measures, they would not have shared their information and content with Facebook to the extent that they did, if at all.

495. Plaintiffs and Class Members were damaged because, as a result of Defendants'

deceit, their content and information have been disclosed to third parties without their consent. Plaintiffs and Class Members were also damaged because, as a result of Defendants' deceit, their privacy was invaded. Plaintiffs and Class Members are at heightened risk of identity theft, phishing schemes, and other malicious attacks. Due to Defendants' deceit, Plaintiffs' and Class Members' information and content were compromised, and may be available on the dark web or in the hands of foreign nationals. Plaintiffs are therefore entitled to "any damage" that they have suffered under Civil Code Section 1709.

496. **Second**, Defendants have committed deceit by failing to meaningfully disclose to Plaintiffs and Class Members how Facebook allows other third parties—including but not limited to app developers, device makers, mobile carriers, software makers, and others—to obtain their personal information notwithstanding their privacy settings.

497. Defendants misled users to believe that they were protecting users' privacy and failed to disclose that they were sharing users' content and information with third parties.

498. Defendants did not disclose that, notwithstanding privacy settings that purported to provide Plaintiffs with control over their content and information, Facebook allowed third-parties to harvest and store personal information.

499. Defendants had a duty to provide accurate information to Plaintiffs about how their content and information were disclosed to third parties by Facebook. Defendants knew that Plaintiffs shared personal and sometimes intimate details about their lives, personalities, and identities. Defendants encouraged Plaintiffs to share content and information by assuring them that Facebook would respect their choices concerning privacy.

500. Defendants intentionally concealed and omitted material information regarding how Facebook disclosed Plaintiffs' content and information in an effort to create a false sense of security and privacy for Plaintiffs and Class Members. Defendants did this because they wanted Plaintiffs to provide more detailed content and information, whose value would be increased by that additional detail. Third parties would thereby pay a higher price for access to that content and information, increasing Facebook's revenue.

501. Had Plaintiffs and Class Members been aware of the full extent of how Facebook collected and used their content and information, they would not have shared their content and information on their devices on the Facebook platform to the same degree that they did, if at all.

502. Plaintiffs and Class Members were damaged because their content and information were disclosed to third-party device makers and other business partners without their consent. As a result of the disclosures of Plaintiffs' and Class Members' content and information to these third parties, Plaintiff could not take remedial measures to protect themselves from identity theft, scams, phishing, unwanted political targeting, even surveillance and other forms of harassment. Moreover, Plaintiffs would have behaved differently and shared less content and information had these acts been disclosed. Facebook deliberately withheld notice because it did not want to discourage user sharing and engagement on its platform.

503. **Third**, Defendants failed to disclose to Plaintiffs and Class Members how their content and information was being collected, shared and aggregated to develop digital profiles or dossiers of each user. Those dossiers, comprised of Facebook user content and information was combined with other sources to de-anonymize this data such that Facebook users could be individual targeted.

504. Defendants had a duty to disclose the full extent to which it allowed Plaintiffs and Class Members to be targeted by advertisers and marketers because it promised in its Contracts that it would not share users' content and information with advertisers without their consent. Defendants' duty also arose from its affirmative representations that (1) Plaintiffs could control their content and information, and (2) third parties could not access personal data absent users' consent.

505. Defendants knew that advertisers were targeting Plaintiffs and Class Members with messages based upon Facebook-derived content and information, combined with content and information derived from other data brokers. Facebook was the vehicle to target Plaintiffs and Class Members by drawing upon the vast amounts of content information collected by Facebook and "matched" with additional information collected about them by data brokers.

506. Defendants knew that psychographic marketing and other targeted advertising was very lucrative, and that advertisers paid a premium to combine content and information with data from data brokers.

507. Defendants did not disclose to Plaintiffs and Class Members that advertisers were combining data from data brokers with Facebook-derived content and information to target them with advertisements and psychographic marketing, as well as building digital dossiers of users.

508. Defendants intended to deceive Plaintiffs and Class Members about their vulnerability to targeted advertisements. Defendants intended to deceive Plaintiffs and Class Members about the degree to which sharing their information and content on Facebook directly led to targeted messaging.

509. Had Plaintiffs and Class Members known the extent to which Defendants shared their content and information with third parties, and how it was aggregated and made available to advertisers and political operatives, among others, Plaintiffs and Class Members would have not shared their information and content on Facebook to the extent that they did, if it all.

510. Plaintiffs and Class Members suffered injury as a direct result of Defendants' deceit. Plaintiffs and Class Members conferred a benefit on Defendants. Their information and content were used and aggregated by advertisers and other third parties without their consent, and for nefarious—among other—uses, and Facebook received substantial advertising revenues as a benefit. Had Plaintiffs and Class Members known the extent and degree to which their content and information was provided to third parties, they would have required compensation for this use of their content and information.

511. As a result, Defendants have been unjustly enriched by its deceit, and Plaintiffs and Class Members are entitled to restitution. "Restitution is a remedy that may be awarded to prevent unjust enrichment when the defendant has obtained some benefit from the plaintiff through fraud, duress, conversion or similar misconduct." *McBride v. Boughton*, 123 Cal.App.4th 379, 387–388 (2004).

512. For all types of fraudulent omissions complained of here, Plaintiffs and Class

Members seek disgorgement of Facebook's profits that were made with the use of Plaintiffs' and Class Members' content and information. Disgorgement is appropriate because Defendants profited from Plaintiffs' and Class Members' content and information wrongfully obtained by generating revenues from app developers and advertisers. Disgorgement is necessary in order to deter future unauthorized use of Plaintiffs' and Class Members' content and information. Disgorgement is also necessary to the extent that the value of Plaintiffs' and Class Members' content and information cannot be assessed by ordinary tort damages. Public policy supports the use of disgorgement here to disincentivize the type of deception that Facebook used in exploiting Plaintiffs' and Class Members' content and information.

**Claim IV. Invasion of Privacy – Intrusion into Private Affairs  
(Against Prioritized Defendant Facebook and Doe Defendants; Non-Prioritized Defendants  
Zuckerberg, Mercer, Bannon and Kogan)  
On Behalf of All Plaintiffs and All Classes**

513. Plaintiffs incorporate by reference all allegations of this complaint as though fully set forth herein.

514. Plaintiffs and Class Members reasonably expected that the content and information that they entrusted to Facebook would be protected and secured against access by unauthorized parties and would not be disclosed to or obtained by unauthorized parties, or disclosed or obtained for any improper purpose.

515. Defendants intentionally intruded upon the private affairs and concerns of Plaintiffs and Class Members by improperly accessing and obtaining Plaintiffs' and Class Members' content and information and using it for improper purposes, as detailed herein.

516. Facebook intentionally intruded upon the private affairs and concerns of Plaintiffs and Class Members, by making Plaintiffs' and Class Members' content and information available to unauthorized parties, including but not limited to third parties including but not limited to device makers, mobile carriers, software makers, security firms, app developers, disclosing this information to unauthorized parties, and failing to adequately protect and secure this information against access by unauthorized parties.

517. Defendants' intrusions upon the private affairs and concerns of Plaintiffs and



Class Members were substantial, and would be highly offensive to a reasonable person, as is evidenced by the intense public outcry and numerous, international governmental investigations in response to Defendants' invasions of Plaintiffs' and Class Members' privacy rights.

518. Plaintiffs and Class Members did not consent to Defendants' intrusions upon their private affairs and concerns.

519. Plaintiffs and Class Members suffered actual and concrete injury as a result of Defendants' intrusions upon Plaintiffs' and Class Members' private affairs and concerns.

520. Plaintiffs and the Class seek appropriate relief for that injury, including but not limited to damages that will reasonably compensate Plaintiffs and Class Members for the harm to their privacy interests, risk of future invasions of privacy, and the mental and emotional distress caused by Defendants' invasions of privacy, as well as disgorgement of profits made by Defendants as a result of their intrusions upon Plaintiffs' and Class Members' private affairs and concerns.

**Claim V. Invasion of Privacy – Public Disclosure of Private Facts  
(Against Prioritized Defendant Facebook and Doe Defendants; Non-Prioritized Defendants  
Zuckerberg, Mercer, Bannon and Kogan)  
On Behalf of All Plaintiffs and All Classes**

521. Plaintiffs incorporate by reference all allegations of this complaint as though fully set forth herein.

522. As detailed herein, Facebook published private content and information of Plaintiffs and Class Members to unauthorized parties, including Facebook's third party partner device makers, mobile carriers, software makers, security firms, including millions of app developers, and failed to take reasonable steps to prevent further dissemination of this content and information.

523. Facebook's publication of Plaintiffs' and Class Members' content and information would be highly offensive to a reasonable person, as is evidenced by the intense public outcry and numerous, international governmental investigations in response to Facebook's invasion of Plaintiffs' and Class Members' privacy rights, and decreased participation on the Facebook platform. Facebook knew or acted with reckless disregard of the fact that a reasonable

person would consider Facebook's publication of Plaintiffs' and Class Members' content and information to be highly offensive.

524. Plaintiffs' and Class Members' content and information was private and not of legitimate public concern or substantially connected to a matter of legitimate public concern.

525. Plaintiffs and Class Members suffered injury as a result of Defendants' publication of Plaintiffs' and Class Members' content and information. They seek appropriate relief, including but not limited to damages that will reasonably compensate Plaintiffs and Class Members for the harm to their privacy interests and the mental and emotional distress caused by Defendants' invasions of privacy, as well as disgorgement of profits made by Facebook as a result of its publication of Plaintiffs' and Class Members' content and information.

**Claim VI. Breach of Contract  
(Against Prioritized Defendant Facebook, Inc.)  
On Behalf of All Plaintiffs and All Classes**

526. Plaintiffs incorporate by reference all allegations of this complaint as though fully set forth herein.

527. At all relevant times, Facebook and Plaintiffs mutually assented to, and therefore were bound by the version of Facebook's Statement of Rights and Responsibilities or later, the Terms of Service, (collectively, the "Contracts") that was operative at the time each of the Plaintiff and Class Member joined Facebook.

528. Throughout the Class Period, Facebook affirmatively stated that Facebook would "not share your content and information with advertisers without your consent." None of the Contracts informed and obtained users' meaningful and lawfully-obtained consent to share their content and information with advertisers and other third parties, or disclosed that such information would be shared if users' friends entered into an agreement which permitted third parties to collect their friends' information.

529. Thus, per the provision above, the Contracts did not authorize Facebook to share Plaintiffs' and Class Members' content and information with Facebook's business partners, including but not limited to mobile carriers, software makers, security firms, chip designers or

device makers.

530. Further, per the provision above, the Contracts also did not authorize Facebook to make the content and information that users shared with friends available to third party app developers, or to sell such information to other third parties like Cambridge Analytica. The Contracts did provide that the user's content and information would be shared with a third-party application if the user *himself or herself* permitted an application to have access and agreed to its terms ("user sharing"). The Contracts did *not* provide that a user's content and information would be shared with a third-party application if a friend of the user used such an application ("friend-of-user sharing"). At the very least, friend-of-user sharing fell outside the scope of the sharing allowed by the Contracts.

531. Facebook's Privacy Policy, and later, its Data Use Policy, were not incorporated into the the Contracts. Indeed, Facebook has previously represented that it is not contractually bound by its Privacy and Data Use Policies.

532. Between 2005 and the present, Facebook has unilaterally drafted at least 80 different policies and user agreements. Upon information and belief, Facebook, in many instances, failed to notify users of updates to these policies. Due to Facebook's failure to provide notice, users could not give consent to these updates to the policies or authorize any acts premised upon such changes.

533. Additionally, Facebook made it unreasonably difficult for users to access the provisions of the Privacy and Data Use Policies, and particularly the provision of the Privacy and Data Use Policies disclosing friend-of-user sharing.

534. Facebook also made it unreasonably difficult for users to understand which privacy settings governed how third-party applications and advertisers could access users' content and information via friend-of user sharing.

535. During the Class Period, Facebook failed to adequately explain that a user's "Privacy settings" were ineffective in controlling whether users' content and information was shared via friend-of-user sharing.

536. Additionally, Facebook failed to adequately explain that multiple default privacy settings, which changed over time, required users to opt *out* of permitting app developers to obtain content and information via friend-of-user sharing. Indeed, Facebook could have, but did not, provide a hyperlink to all of the pages which required users to visit and authorize such sharing. Instead, those pages contained default settings which assumed sharing. Such default settings, undisclosed to users, did not authorize or grant consent for sharing with third parties.

537. GSR made an application available to Facebook users via Graph API v.1.0. It used Graph API v.1.0 to collect sensitive information regarding Plaintiffs—information that personally identified, or could easily be used to personally identify, Plaintiffs.

538. Facebook was informed that GSR then sold this information to Cambridge Analytica, which used the information to craft and target advertising on Facebook’s platform to Plaintiffs and Class members. This was prohibited by the Contracts.

539. Upon information and belief, during the Class Period, certain Doe Defendants made applications available to Facebook users to collect sensitive information regarding Plaintiffs and the Class. Upon information and belief, certain Doe Defendants also sold users’ content and information to advertisers, thus causing a violation of the Contracts.

540. Contrary to the Contracts, Facebook knowingly allowed Doe Defendants who made their applications available through Graph API v.1.0 to sell the personally identifiable information regarding Plaintiffs and the Class that they had collected via applications that used the Facebook platform.

541. The Contracts required Facebook to protect the content and information of its users. The Contracts affirm that users’ content and information would not be shared with advertisers and other third parties without their affirmative consent. Likewise, these same terms of service informed users that their privacy setting would control who had access to their content and information, but this was untrue. Facebook did not disclose that users were required to affirmatively “opt out” of sharing their content and information with third parties in the Contracts.

542. As set forth herein, Plaintiffs' content and information is of considerable value as demonstrated by Facebook's calculation of the Average Revenue Per User that it calculates. There is an active market for the content and information generated by Facebook users, both individually and especially in the aggregate. Facebook generates billions of dollars in revenues through targeted advertising delivered to third parties, curated through the collection and aggregation of Facebook's user data. There is also an active black market for user content and information. The remedy for the breach of the Contracts is what Facebook gained through their breach.

543. The value of the content and information accumulated by Facebook about a user increases with the amount of content and information Facebook collects. Thus, over time, Facebook's benefit of the bargain has multiplied dramatically.

544. As a result of the breach, Plaintiffs have been harmed and have suffered damages by losing the value of their content and information.

**Claim VII. Negligence and Gross Negligence  
(Against Prioritized Defendant Facebook, Inc., and Doe Defendants)  
On Behalf of All Plaintiffs and Classes**

545. Plaintiffs incorporate by reference all allegations of this complaint as though fully set forth herein.

546. Plaintiffs bring this claim on behalf of themselves and the Nationwide Class.

547. Defendants owed a duty to Plaintiffs and the Class to exercise reasonable care in the obtaining, using, and protecting of their content and information, arising from the sensitivity of their content and information and the expectation that their content and information was not going to be shared with third parties without their consent. This duty included Facebook ensuring that no app developers, device makers or other third parties, including Kogan, GSR and Cambridge Analytica, were improperly collecting, storing, obtaining and/or selling Plaintiffs' and Class members' content and information.

548. Plaintiffs' and Class members' willingness to entrust Defendants with their content and information was predicated on the understanding that Facebook would take

appropriate measures to protect it. Facebook had a special relationship with Plaintiffs and Class members as a result of being entrusted with their content and information, which provided an independent duty of care.

549. Facebook knew that the content and information of Plaintiffs and the Class had value. Indeed, Facebook has earned billions of dollars from selling targeted advertising on its platform based on users' content and information as demonstrated by Facebook's calculation of the Average Revenue Per User. There is an active market for the content and information generated by Facebook users, both individually and especially in the aggregate. Facebook generates its billions of dollars in revenues through targeted advertising delivered to third parties, curated through the collection and aggregation of Facebook's users' content and information. There is also an active black market for user content and information.

550. Facebook received multiple warnings that Plaintiffs' and the Class Members' content and information was at risk.

- (5) In 2012, Sandy Parakilas, former Facebook operations manager, warned Facebook's executives about the risks of app developers gaining access to users' personal information without their consent on Facebook's platform. Yet, Facebook ignored Parakilas's warnings.
- (6) In October 2012, Facebook reached a settlement with the FTC agreeing to clearly and prominently disclose its sharing of information with third parties; yet, Facebook continued to let app developers access users' information without their consent.
- (7) As late as 2017, Alex Stamos, Facebook's former Chief of Security, warned Facebook executives about security risks on the platform. In an internal meeting held in 2017, Stamos warned of "intentional decisions to give access to data and systems to engineers to make them 'move fast' but that creates other issues for us."
- (8) In 2017, Stamos states that he provided a written report concerning the circumstances leading to Cambridge Analytica obtaining users' personal

information. Facebook edited and published a whitewashed version of this report concealing any wrongdoing.

551. Despite these warnings, Facebook failed to take reasonable steps to prevent harm to Plaintiffs:

- (1) According to Sandy Parakilas, Facebook was not conducting regular audits of app developers using Facebook's platform in 2012.
- (2) On April 30, 2014, Facebook announced a new "anonymous login" feature that would have allowed users to use an app without sharing any personal information. Yet, Facebook never implemented this feature.
- (3) On April 30, 2014, Facebook also announced a new "controlled login" feature to allow users to choose what information they shared with app developers before login in. Yet, Facebook did not implement this feature until May 2015.
- (4) As early as December 11, 2015, Facebook received notice that app developer Aleksandr Kogan had shared users' personal information with Cambridge Analytica; yet, Facebook waited until April 2018, more than three years later, to notify users that their personal information had been improperly shared.

552. Facebook owed a duty to timely disclose to Plaintiffs and Class member that Facebook had allowed their content and information to be accessed by GSR, Cambridge Analytica and the Doe Defendants. Plaintiffs had a reasonable expectation that Facebook would inform them of the improper disclosure of their content and information.

553. Facebook breached its duties by, among other things: (a) failing to ensure that app developers, device makers and other third parties were not improperly collecting, storing, obtaining and/or selling Plaintiffs' and the Class' content and information without users' informed consent; and (b) failing to provide adequate and timely notice that Plaintiff's and Class members' content and information had been improperly obtained by Cambridge Analytica and Doe Defendants.

554. But for Facebook's breach of its duties, including its duty to use reasonable care



to protect and secure Plaintiffs' and Class members' content and information, Plaintiffs' and Class members' content and information would not have been disclosed without their consent to third parties, which resulted in further misuse of Plaintiffs' and Class members' content and information.

555. Plaintiffs and Class members were foreseeable victims of Facebook's breach of its duties. Facebook knew or should have known that allowing third parties to access Plaintiffs' and Class members' content and information would cause damage to Plaintiffs and Class members.

556. As a result of Facebook's negligent failure to safeguard Plaintiffs' and Class members' content and information, Plaintiffs and Class members have suffered injury, which includes but is not limited to impermissible disclosure of their content and information, both directly and indirectly by Facebook, and exposure to a heightened, imminent risk of misuse, fraud, identity theft, voter fraud, medical fraud, and financial and other harms.

557. The content and information shared with third parties allows this content and information to be aggregated with other data to identify and target Plaintiffs and Class members. It is reasonable for Plaintiffs and Class Members to obtain identity protection or credit monitoring services in light of the foregoing. Plaintiffs seek to recover the cost of these services from Facebook.

558. The injury to Plaintiff and Class Members was a proximate, reasonably foreseeable result of Facebook's breaches of its aforementioned duties.

559. As a proximate result of Facebook's negligence in failing to take due care to monitor the use of user content and information by third parties like mobile device makers, carriers, software makers, security firms, chip designers, GSR and Doe Defendants, Plaintiffs suffered damages in an amount to be proved at trial.

560. Public policy voids any purported waiver of liability to which Facebook may claim Plaintiffs assented:

A. The contract(s) between Facebook and Plaintiffs concern a business of a

type generally thought suitable for public regulation; indeed, Facebook is subject to public regulation.

B. Due to Facebook's ubiquity and importance in the daily lives of Americans, it performs a service of great importance to the public. Using Facebook is often a matter of practical necessity for the many persons who use Facebook to coordinate daily activities, network, engage in political and cultural discourse, and pursue interests and hobbies. To do these things, Facebook users must share their personal information with their friends.

C. Facebook holds itself out as a free provider of its services to aged 13 or above.

D. Because of the network effect and the importance of Facebook's services, Facebook possesses a decisive advantage of bargaining strength against any member of the public that seeks to use its services.

E. Any purported waiver of liability occurs in a standardized adhesion contract that users must accept or reject in toto.

F. Facebook is ultimately in total control of its platform and services. The confidentiality of Plaintiffs' personal information, therefore, is under Facebook's control and subject to its carelessness.

561. In addition, any purported waiver of liability is unconscionable.

562. Facebook's conduct also constitutes gross negligence due to its extreme departure from ordinary standards of care, and its knowledge that it had failed to secure the content and information of Plaintiffs and Class Members.

**Claim VIII. Violations of the California Unfair Competition Law**  
**Cal. Bus. & Prof. Code §§ 17200 *et seq.***  
**(Against Prioritized Defendant Facebook and Doe Defendants; Against Non-Prioritized**  
**Defendants Zuckerberg, Mercer, Bannon and Kogan)**  
**On Behalf of All Plaintiffs and Classes**

563. Plaintiffs incorporate by reference all allegations of this complaint as though fully set forth herein.

564. Plaintiffs bring this claim on behalf of themselves and the Nationwide Class.

565. Defendants' conduct as alleged herein constitutes unfair, unlawful, or fraudulent business acts or practices as proscribed by California's Unfair Competition Law, Cal. Bus. & Prof. Code § 17200, et seq. ("UCL").

566. As alleged above, Facebook violated Plaintiffs' and Class members' privacy by allowing their personal content to be exploited in ways that Plaintiffs and Class members could not have been anticipated. Plaintiffs and Class Members' interests were also violated through Defendants' deceptive acts. Had Plaintiffs and Class members known the extent to which Facebook allowed their personal content to be collected, aggregated, pooled, and transferred for commercial purposes to companies such as Cambridge Analytica, Plaintiffs and Class members would not have shared their content and information on Facebook to the same extent they did, if at all. Facebook allowed app developers, device makers and other third parties to harvest users' friends content and information on a large scale, with no effective notice to Plaintiffs and Class Members, and without any opportunity for Plaintiffs and Class Members to become reasonably informed about Facebook's default privacy settings allowing app developers, device makers and other third parties to harvest users' friends content and information or the risks that large-scale disclosure of their content and information would present. Facebook made assurances to Plaintiffs and Class members about respecting their privacy, and being able to own and control their content and information. Given these affirmative statements, Facebook had a duty to disclose the nature and extent of the uses of users' content and information that Facebook allowed app developers, device makers, and other third parties to make.

567. **Defendants' conduct is "unfair."** California has a strong public policy to protect privacy interests, including in protecting the content and information shared by Plaintiff. Defendants violated this public policy by exploiting Plaintiffs' content and information without informed consent.

568. Defendants' conduct also violated the interests protected by the Video Privacy Protection Act, 18 U.S.C. § 2710; the Stored Communications Act, 18 U.S.C. § 2701 *et seq.*;

Cal. Civ. Code §§ 1709 & 1710 and Article 1, § 1 of the California Constitution. To establish liability under the unfair prong, Plaintiffs need not establish that these statutes were actually violated, although the claims pleaded herein do so.

569. Facebook did not reasonably inform Plaintiffs of the uses of their content and information, and invaded Plaintiffs' and Class members' privacy by subjecting their content and information to large-scale disclosure without knowledge or meaningful consent. Class Members could not have anticipated this degree of intrusion into their privacy, which included exposure to psychographic marketing. Defendants' conduct did not create a benefit that outweighs these strong public policy interests. Defendants' conducts narrowly benefitted Facebook and its business partners at the expense of the privacy of millions of people. Additionally, the effects of Facebook's conduct were comparable to or substantially the same as the conduct forbidden by the California Constitution and the common law's prohibitions against invasion of privacy, in that Facebook's conduct invaded fundamental privacy interests.

570. **Defendants' conduct is "unlawful."** Defendants' conduct violates the Video Privacy Protection Act, 18 U.S.C. § 2710; the Stored Communications Act, 18 U.S.C. § 2701 *et seq.*; Cal. Civ. Code §§ 1709 and 1710; and Article 1, § 1 of the California Constitution.

571. Facebook's conduct violated the spirit and letter of these laws, which protect privacy interests and prohibit misleading and deceptive practices. The content and information that Facebook allowed third parties to harvest exposed Plaintiffs and Class Members to an increased risk of identity theft, voter fraud, tax return fraud, and allowed third parties to link their identities to other data in order to de-anonymize them.

572. **Defendants' conduct is fraudulent.** As alleged above, Defendants misled Plaintiffs concerning the use of their content and information affirmatively and through material omissions, and the privacy protection Facebook provided their content and information. Defendants did not meaningfully disclose that Plaintiffs' content and information could be obtained by device makers, notwithstanding Plaintiffs' privacy settings. Defendants did not disclose that Facebook's default privacy settings allowed third party apps to obtain their content

and information, and obfuscated how Plaintiffs could have protected their content and information from disclosure to third parties. Defendants omitted material information about how Plaintiffs' personal content was harvested, stored, searched, used and sold.

573. Plaintiffs and Class Members have suffered injury in fact and lost money or property due to Defendants' business acts or practices. Plaintiffs' content and information has tangible value. Plaintiffs' content and information is in the possession of third parties who have used and will use it for their own advantage, including financial advantage, or have sold it or will sell it for value, making it clear that Plaintiffs' content and information has tangible value.

574. Plaintiffs and Class members are at increased risk of identity theft due to Facebook's practices concerning sharing users' content and information with third parties. Plaintiffs may be subjected to voter fraud, identity theft, medical fraud, and other harms. The content and information shared with third parties allows this content and information to be aggregated with other data to identify and target Plaintiffs and Class Members. It is reasonable for Plaintiffs and Class Members to obtain identity protection or credit monitoring services in light of the foregoing. Plaintiffs seek to recover the cost of these services from Facebook.

575. Defendants invaded Plaintiffs' privacy by failing to inform Plaintiffs and Class Members that Facebook was sharing their content and information with its business partners, including but not limited to app developers, mobile carriers, software makers, security firms, device makers and chip designers.

576. Defendants further failed to inform Plaintiffs and Class members about the nature of the app developers' business, or the purposes for which app developers were obtaining their content and information. Facebook did not disclose the nature or the extent of the exploitation of Plaintiffs' content information. Facebook invaded Plaintiffs' and Class Members' privacy by subjecting them to psychographic marketing that exploited intimate aspects of their identity, including emotional and psychological manipulation.

577. Plaintiffs' and Class members' content and information was exploited without informed consent. Accordingly, Plaintiffs are entitled to part of Facebook's profits that were

generated by their content and information without informed consent.

578. Plaintiffs and Class members seek an order to enjoin Defendants from such unlawful, unfair, and fraudulent business acts or practices, and to restore to Plaintiffs and Class members their interest in money or property that may have been acquired by Defendants by means of unfair competition.

579. Section 17203 of the UCL authorizes a court to issue injunctive relief “as may be necessary to prevent the use or employment by any person of any practice which constitutes unfair competition.” Plaintiffs and Class members also seek the following injunctive relief: (1) an “opt in” rather than “opt out” default for sharing personal content in all of Facebook’s user settings; (2) disclosure of the purposes of which Plaintiffs’ personal content is used by Facebook, data brokers, device makers, mobile carriers, software makers, security firms, app developers, advertisers and other third parties with whom Facebook has shared users’ content and information without their consent; (3) destruction of all personal content obtained by Defendants and all such third parties where such content is within Defendants’ control or possession; (4) a complete audit and accounting of the uses of Plaintiffs’ and Class Members’ content and information by app developers, device makers, and other business partners; (5) a permanent injunction preventing such sharing of content and information with these third parties without Facebook users’ informed consent and affirmative authorization; and (6) a permanent ban on targeting Plaintiffs and class members with advertisements or marketing materials based on information from data brokers.

**Claim IX. Violation of Article I, Section 1 of the California Constitution  
(Against Prioritized Defendant Facebook and Doe Defendants; Against Non-Prioritized  
Defendants Zuckerberg, Mercer, Bannon and Kogan)  
On Behalf of All Plaintiffs and All Classes**

580. Plaintiffs incorporate by reference all allegations of this complaint as though fully set forth herein.

581. Plaintiffs bring this claim on behalf of themselves and the Nationwide Class.

582. The California Constitution expressly provides for a right to privacy: “All people are by nature free and independent and have inalienable rights. Among these are enjoying and

defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy.” Cal. Const., art. I, § 1

583. Plaintiffs have a privacy right at issue. Plaintiffs and Class Members have an interest in preventing the unauthorized disclosure and misuse of their content and information and in conducting their personal activities without intrusion or interference, including the right to not to have their content and information used by Cambridge Analytica and other third parties for these parties’ benefit, or against Plaintiffs’ interests.

584. Facebook promised that Plaintiffs’ content and information was their property, and that it would respect their privacy settings, but Facebook did not do so. Facebook did not provide Plaintiffs the opportunity to give their informed consent regarding the uses of their content and information, and allowed a feature where users’ content and information could be shared by their friends’ participation in an application notwithstanding users’ privacy elections. Facebook’s conduct affected millions of users, including Plaintiffs.

585. Facebook knew about Plaintiffs’ vulnerability to having their content and information exploited, and intended for these uses to occur without Plaintiffs’ knowledge or consent. Facebook intentionally misled users about the efficacy of their privacy settings. As alleged above, Facebook violated Plaintiffs’ and Class members’ privacy by allowing their content and information to be exploited in ways that Plaintiffs and Class members could not have been anticipated. Had Plaintiffs and Class members known the extent to which Facebook allowed their content and information to be collected, aggregated, pooled, and transferred for commercial purposes to companies such as Cambridge Analytica, Plaintiffs and Class members would not have shared their content and information on Facebook to the same extent they did, if at all. Facebook allowed app developers to harvest users’ friends content and information on a large scale, with only the most minimal of notice to Plaintiffs and Class members. This notice did not remotely inform Plaintiffs of the full extent of the uses of their content and information. Facebook made assurances to Plaintiffs and Class members about respecting their privacy, and being able to own and control their content and information. Given these affirmative statements,



Facebook had a duty to disclose the nature and extent of the uses of their content and information that Facebook allowed app developers, device makers, and other third parties to make.

586. Facebook misled Plaintiffs and Class Members about the privacy of their content and information, including that photographs and other content and information shared by Plaintiffs and Class Members would be “private,” or shared only with their Facebook friends, when in fact this content and information was shared directly with app developers and other business partners through Facebook’s API. Indeed, Facebook took measures to prevent the privacy settings on photographs from being recognized by third parties that were using API feeds.

587. Facebook’s publication of Plaintiffs’ and Class Members’ content and information would be highly offensive to a reasonable person, as is evidenced by the intense public outcry and numerous, international governmental investigations in response to Facebook’s invasion of Plaintiffs’ and Class members’ privacy rights, and decreased participation on the Facebook platform even though the entire scope of the breach has yet to be revealed.

**Claim X. Violation of California Common Law Right of Publicity  
(Against Prioritized Defendant Facebook and Doe Defendants; Against Non-Prioritized  
Defendants Zuckerberg, Mercer, Bannon and Kogan)  
On Behalf of All Plaintiffs and Classes**

588. Plaintiffs incorporate by reference all allegations of this complaint as though fully set forth herein.

589. Plaintiffs bring this claim on behalf of themselves and the Nationwide Class

590. California common law prohibits the use of a person’s name or likeness for the defendant’s advantage, commercial or otherwise, without first obtaining that person’s consent.

591. Facebook violated this section by allowing access to Plaintiffs’ and Class Members’ likeness—including names, like history, photographs, and video—as a service to third parties. On information and belief, access to the likeness of Plaintiffs and Class Members was integral to the services Facebook offered app developers like Cambridge Analytica. App developers would not have purchased services from Facebook (including advertisements) without access to this information. Indeed, the value of the services Facebook offered to app

developers was derived from this information.

592. Prior to using the Plaintiffs' likeness, Facebook never obtained consent from the Plaintiffs.

593. Plaintiffs did not receive any compensation in return for this use

594. Plaintiffs were harmed by Facebook's improper use.

595. Plaintiffs seek actual damages suffered, plus any profits attributable to Facebook's use of the unauthorized use not calculated in actual damages. Plaintiffs also reserve the right to punitive damages, costs, and reasonable attorney's fees as allowed under this statute.

**Claim XI. Breach of the Implied Covenant of Good Faith and Fair Dealing  
(Against Defendant Facebook)**

596. Plaintiffs incorporate by reference all allegations of this complaint as though fully set forth herein.

597. Under California law, there is in every contract or agreement an implied promise of good faith and fair dealing. Such a duty is read into contracts and functions as a supplement to the express contractual covenants, in order to prevent a transgressing party from engaging in conduct which (while not technically transgressing the express covenants) frustrates the other party's rights to the benefit of the contract. Thus, any claim on the part of Facebook that technically it was permitted to allow the collection and transmittal of Plaintiffs' and the putative class's data, must be read in the context of, and give way to, those users' rights to the benefit of the contract, including the terms strictly delimiting such activity.

598. Facebook entered into a Statement of Rights and Responsibilities with Plaintiffs and Class Members.

599. A covenant of good faith and fair dealing attaches to Facebook's Statement of Rights and Responsibilities.

600. In its Statements of Rights and Responsibilities, Facebook promised Plaintiffs and Class Members that "We do not give your content or information to advertisers without your consent."

601. Facebook also promised “[y]our privacy is very important to us,” and that Plaintiffs and Class Members could control their content and information because they “own all of the content and information [they] post on Facebook, and [they] can control how it is shared through your privacy and application settings.”

602. Plaintiffs and Class Members did all they were required to do under these contractual provisions.

603. Under the terms of the Statement of Rights and Responsibilities, Plaintiffs and Class Members were entitled to receive the benefits promised to them by Facebook, including that Facebook would protect the privacy of their user content and information, would not disclose user content and information to third parties without the user’s consent, and would keep user content and information secure.

604. Facebook was uniquely able to control the rights of its users, including Plaintiffs’ and Class Members’, concerning their privacy, ownership and control of their content and information, and whether their content and information would be provided to advertisers, device makers, and/or third parties without consent.

605. Facebook surreptitiously took measures to frustrate and undercut Plaintiffs’ and Class Members’ contractual rights concerning their privacy, ownership and control over their content and information, and whether their content and information would be provided to advertisers without consent. By doing so, Facebook deprived Plaintiffs and Class Members of the benefits under their contracts with Facebook, including the Statements of Rights and Responsibilities.

606. Facebook entered into business relationships with app developers, device makers, big companies such as Amazon and Qualcomm, and other third parties that allowed Plaintiffs’ and Class Members’ content and information to be transmitted without the user’s consent.

607. By disclosing, publishing, and providing Facebook users’ content and information to advertisers without informing Plaintiffs and Class Members, Facebook breached the covenant of good faith and fair dealing. Facebook allowed its users to be targeted by advertisements,

including psychographic marketing, without seeking consent of Plaintiffs or Class Members, and did not allow Plaintiffs and Class Members to make informed decisions about sharing their content and information on Facebook's platform. This unfairly interfered with Plaintiffs' and Class Members' rights under the Statement of Responsibilities to have their user content and information kept secure and private and not disclosed to third parties without the their consent.

608. Additionally, by failing to secure Plaintiffs' and Class Members' content and information, and by taking measures to ensure that Plaintiffs' and Class Members' privacy settings and reasonable expectations of privacy were not recognized or honored, including by disclosing and publishing user content and information through Facebook's API streams sent to app developers, device makers, and other third parties, Facebook deprived Plaintiffs and Class Members of the benefits of their agreements.

609. Plaintiffs and Class Members were damaged by Facebook's breaches of its duty of good faith and fair dealing. Plaintiffs and the Class members did not receive the benefit of the bargain for which they contracted. Plaintiffs and Class Members suffered invasions of privacy and were directly targeted by advertisers without their consent, including by Cambridge Analytica. Plaintiffs and Class Members' content and information was released, disclosed, published and, and they are at risk of identity theft. In this regard, Facebook failed to secure Plaintiffs' and Class Members' content and information and shifted the burden of doing so from Facebook to Plaintiffs and Class Members.

**Claim XII. Quantum Meruit to Recover Sums Had by Unjust Enrichment  
(Against Prioritized Defendants Facebook, Zuckerberg and Doe Defendants)  
On Behalf of All Plaintiffs and All Classes**

610. Plaintiffs reallege and incorporate by reference all allegations of this complaint as though fully set forth herein. This claim is pleaded in the alternative to the claims for breach of contract.

611. Because no adequate legal remedy is available under any applicable contract, Plaintiffs bring this count in quasi contract on behalf of themselves and Class Members in order to pursue restitution based on Facebook's unjust enrichment, including by way of Defendants'

retention of profits that should have been expended to protect the data of Plaintiffs and Class Members per its published privacy agreements and policies.

612. As alleged herein, Defendants have unjustly received and retained monetary benefits from Plaintiffs and Class Members—*i.e.*, by way of its use of, and profiting from, their data under unjust circumstances, such that inequity has resulted.

613. By engaging in the conduct described in this complaint, Defendants knowingly obtained benefits from Plaintiffs and Class Members as alleged herein under circumstances such that it would be inequitable and unjust for Facebook to retain them.

614. More specifically, by engaging in the acts and failures to act described in this complaint, Defendants have been knowingly enriched by the savings in costs that should have been reasonably expended to protect the data of Plaintiffs and Class Members. Defendants were on notice that gathering and transmittal of user data could happen, including by way of previous occurrences and claims brought against it by the FTC, yet it failed to take reasonable steps to pay for the level of security required to have prevented such unauthorized access, gathering, and transmittal to third parties.

615. Also, Facebook has been enriched unjustly by the use of Plaintiffs' and Class Members' content and information, and has profited greatly as a result, even though it did not protect this data as it had promised. Indeed, Defendants' failure to protect this content and information fueled Defendants' enrichment. Encouraging Plaintiffs and Class Members to share their content and information allowed Defendants to collect more such information and aggregate it, to target them more precisely.

616. By engaging in the conduct described in this complaint, Defendants have knowingly obtained benefits from or by way of Plaintiffs and Class Members, including by way of the use of their personal information in the course of its business, including their lucrative data broker business, under circumstances such that it would be inequitable and unjust for it to retain them.

617. Thus, Defendants will be unjustly enriched if it is permitted to retain the benefits

derived from the unauthorized and impermissible gathering and sharing of Plaintiffs and Class Members' data.

618. Plaintiffs and Class Members are therefore entitled to a restitutionary award in an amount to be determined at trial, or the imposition of a constructive trust upon the monies derived by Facebook by means of the above-described actions, or both as the circumstances may merit to provide complete relief to Plaintiffs and Class Members, whether the sums of monies are those: (a) that it should have devoted to complying with its agreements and policies as they pertain to the user data that is the subject of this lawsuit; or (b) the money it has collected from advertisers and others that corresponds to the user data that is the subject of this lawsuit; or (c) other sums as it may be just and equitable to return to them.

**B. Priority Consumer Protection Act Claims Alleged in the Alternative**

**Claim XIII. Violations of the Alabama Deceptive Trade Practices Act  
Ala. Code §§ 8-19-1 *et seq.* (2018)  
(Against Facebook) (In the Alternative)**

619. The Alabama Plaintiff identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Alabama Subclass, incorporates by reference all allegations of this complaint as though fully set forth herein.

620. Facebook is a "person" as defined by Ala. Code § 8-19-3(5).

621. Facebook's products and services are "goods" and "services" as defined by Ala. Code § 8-19-3(3), (7).

622. Facebook advertised, offered, or sold goods or services in Alabama and engaged in trade or commerce directly or indirectly affecting the people of Alabama as defined by Ala. Code § 8-19-3(8).

623. The Alabama Deceptive Trade Practices Act, Ala. Code §§ 8-19-1 *et seq.*, prohibits unfair, deceptive, false, and unconscionable trade practices.

624. Facebook engaged in unconscionable, false, misleading or deceptive practices in connection with its business, commerce and trade practices in violation of Ala. Code § 8-19-5(27).

625. Facebook's representations and omissions were material because they were likely to deceive reasonable consumers.

626. Facebook intended Plaintiff and the Alabama Subclass members to rely on its misrepresentations, omissions, and other unlawful conduct.

627. Had Facebook disclosed to Plaintiff and the Alabama Subclass members that it misrepresented and omitted material information about the nature of the privacy of user data, users' ability to control how their data was used, and access of user data to third parties, and was otherwise engaged in deceptive, common business practices, Facebook would have been unable to continue in business and it would have been forced to disclose the defects in its privacy protection. Instead, Facebook represented that its services were protecting user privacy and that users could control the use of the private data. Plaintiff and the Alabama Subclass members acted reasonably in relying on Facebook's misrepresentations and omissions, the truth of which they could not have discovered.

628. Facebook acted intentionally, knowingly, and maliciously to violate Alabama's Deceptive Trade Practices Act, and recklessly disregarded Plaintiff and the Alabama Subclass members' rights.

629. As a direct and proximate result of Facebook's unfair and deceptive acts and practices, Plaintiff and the Alabama Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages.

630. Plaintiff and the Alabama Subclass members have suffered injuries in fact and lost money or property due to Defendant's business acts or practices. Plaintiff's and the Alabama Subclass members' personal content has tangible value. Their personal content is in the possession of third parties who have used and will use it for their own advantage, including financial advantage, or was and is being sold for value, making it clear that the personal content has tangible value.

631. Plaintiff and the Alabama Subclass members are at increased risk of identity theft due to Facebook's practices concerning sharing data with third parties. Plaintiff and the Alabama



Subclass members may be subjected to voter fraud, identity theft, medical fraud, and other harms. The personal content shared with third parties allows personal content to be aggregated with other data to identify and target Plaintiff and the Alabama Subclass members. It is reasonable for Plaintiff and the Alabama Subclass members to obtain identity protection or credit monitoring services in light of the foregoing. Plaintiff and the Alabama Subclass members seek to recover the cost of these services from Facebook.

632. Facebook invaded Plaintiff's and the Alabama Subclass members' privacy by failing to keep them informed about the nature of the app developers' business, or the purposes for which app developers were obtaining their personal content. Facebook did not disclose the nature or the extent of the exploitation of Plaintiff's and the Alabama Subclass members' personal content. Facebook invaded Plaintiff's and the Alabama Subclass members' privacy by subjecting them to psychographic marketing that exploited intimate aspects of their identity, including emotional and psychological manipulation.

633. Plaintiff's and the Alabama Subclass members' personal content was exploited without informed consent. Accordingly, Plaintiff and the Alabama Subclass members are entitled to part of Facebook's profits that were generated by their personal content without informed consent.

634. Written demand for relief has been provided as required under Ala. Code § 8-19-10(e).

635. Plaintiff and the Alabama Subclass seek all monetary and non-monetary relief allowed by law, including the greater of (a) actual damages or (b) statutory damages of \$100; treble damages; injunctive relief; attorneys' fees, costs, and any other relief that is just and proper.

636.

**Claim XIV. Violations of the Colorado Consumer Protection Act  
Colo. Rev. Stat. Ann. §§ 6-1-101 *et seq.*  
(Against Facebook) (In the Alternative)**

637. The Colorado Plaintiff identified above ("Plaintiff," for purposes of this Count),

individually and on behalf of the Colorado Subclass, incorporates by reference all allegations of this complaint as though fully set forth herein.

638. Facebook is a “person” as defined by Colo. Rev. Stat. Ann. § 6-1-102(6).

639. Facebook provides goods and/or services.

640. Plaintiff and Colorado Subclass members, as well as the general public, are actual or potential consumers of the services offered by Facebook to actual consumers.

641. Facebook engaged in deceptive trade practices in the course of its business, in violation of Colo. Rev. Stat. Ann. § 6-1-105(1)(u) by failing to disclose material information concerning its services, including its improper use and lack of protection for private user data, which was known at the time of an advertisement or sale and the failure to disclose this information was intended to induce Plaintiff and the Colorado Subclass to use Facebook’s services.

642. Facebook also engaged in deceptive trade practices in the course of its business, in violation of Colo. Rev. Stat. Ann. § 6-1-105(3) by engaging unfair trade practices actionable at common law or under other statutes of Colorado.

643. Facebook’s representations and omissions were material because they were likely to deceive reasonable consumers to believe their user data could be and was kept private.

644. Facebook intended to mislead Plaintiff and the Colorado Subclass members and induce them to rely on its misrepresentations and omissions.

645. Had Facebook disclosed to Plaintiff and the Colorado Subclass members that it misrepresented and omitted material information about the nature of the privacy of user data, users’ ability to control how their data was used, and access of user data to third parties, and was otherwise engaged in deceptive, common business practices, Facebook would have been unable to continue in business and it would have been forced to disclose the defects in its privacy protection. Instead, Facebook represented that its services were protecting user privacy and that users could control the use of the private data. Plaintiff and the Colorado Subclass members acted reasonably in relying on Facebook’s misrepresentations and omissions, the truth of which

they could not have discovered.

646. Facebook acted fraudulently, willfully, knowingly, or intentionally to violate Colorado's Consumer Protection Act, and with recklessly disregarded Plaintiff and the Colorado Subclass members' rights.

647. As a direct and proximate result of Facebook's deceptive trade practices, Plaintiff and the Colorado Subclass members suffered injuries to their legally protected interests.

648. Plaintiff and the Colorado Subclass members have suffered injuries in fact and lost money or property due to Defendant's business acts or practices. Plaintiff's and the Colorado Subclass members' personal content has tangible value. Their personal content is in the possession of third parties who have used and will use it for their own advantage, including financial advantage, or was and is being sold for value, making it clear that the personal content has tangible value.

649. Plaintiff and the Colorado Subclass members are at increased risk of identity theft due to Facebook's practices concerning sharing data with third parties. Plaintiff and the Colorado Subclass members may be subjected to voter fraud, identity theft, medical fraud, and other harms. The personal content shared with third parties allows personal content to be aggregated with other data to identify and target Plaintiff and the Colorado Subclass members. It is reasonable for Plaintiff and the Colorado Subclass members to obtain identity protection or credit monitoring services in light of the foregoing. Plaintiff and the Colorado Subclass members seek to recover the cost of these services from Facebook.

650. Facebook invaded Plaintiff's and the Colorado Subclass members' privacy by failing to keep them informed about the nature of the app developers' business, or the purposes for which app developers were obtaining their personal content. Facebook did not disclose the nature or the extent of the exploitation of Plaintiff's and the Colorado Subclass members' personal content. Facebook invaded Plaintiff's and the Colorado Subclass members' privacy by subjecting them to psychographic marketing that exploited intimate aspects of their identity, including emotional and psychological manipulation.

651. Plaintiff's and the Colorado Subclass members' personal content was exploited without informed consent. Accordingly, Plaintiff and the Colorado Subclass members are entitled to part of Facebook's profits that were generated by their personal content without informed consent.

652. Facebook's deceptive trade practices significantly impact the public, because Facebook's user platform is used throughout the world, with hundreds of thousands of users who are Colorado residents and consumers.

653. Plaintiff and Colorado Subclass members seek all monetary and non-monetary relief allowed by law, including the greater of: (a) actual damages, or (b) \$500, or (c) three times actual damages (for Facebook's bad faith conduct); injunctive relief; and reasonable attorneys' fees and costs.

**Claim XV. Violations of the Illinois Consumer Fraud and  
Deceptive Business Practices Act  
815 Ill. comp. stat. Ann. §§ 505 *et seq.*  
(Against Facebook) (In the Alternative)**

654. The Illinois Plaintiffs identified above ("Plaintiffs," for purposes of this Count), individually and on behalf of the Illinois Subclass, incorporates by reference all allegations of this complaint as though fully set forth herein.

655. Facebook is a "person" as defined by 815 Ill. Comp. Stat. Ann. § 505/1(c).

656. Plaintiffs and the Illinois Subclass members are "consumer[s]" as defined by 815 Ill. Comp. Stat. Ann. § 505/1(e).

657. Facebook's conduct as described herein was in the conduct of "trade" or "commerce" as defined by 815 Ill. Comp. Stat. Ann. § 505/1(f).

658. Facebook's deceptive, unfair, and unlawful trade acts or practices, in violation of 815 Ill. Comp. Stat. Ann. § 505/2.

659. Facebook's representations and omissions concerning the use of and privacy of user data were material because they were likely to deceive reasonable consumers to believe their user data could be and was kept private.

660. Facebook intended to mislead Plaintiffs and the Illinois Subclass members and

induce them to rely on its misrepresentations and omissions. Plaintiffs and the Illinois Subclass reasonably relied on Facebook's representations about the security of their private data.

661. The above unfair and deceptive practices and acts by Facebook were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury that these consumers could not reasonably avoid; this substantial injury outweighed any benefit to consumers or to competition.

662. Facebook acted intentionally, knowingly, and maliciously to violate Illinois's Consumer Fraud and Deceptive Business Practices Act, and recklessly disregarded Plaintiffs and the Illinois Subclass members' rights.

663. As a direct and proximate result of Facebook's unfair and deceptive acts and practices, Plaintiffs and the Illinois Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in using Facebook's services.

664. Plaintiffs and the Illinois Subclass members have suffered injuries in fact and lost money or property due to Defendant's business acts or practices. Plaintiffs' and the Illinois Subclass members' personal content has tangible value. Their personal content is in the possession of third parties who have used and will use it for their own advantage, including financial advantage, or was and is being sold for value, making it clear that the personal content has tangible value.

665. Plaintiffs and the Illinois Subclass members are at increased risk of identity theft due to Facebook's practices concerning sharing data with third parties. Plaintiffs and the Illinois Subclass members may be subjected to voter fraud, identity theft, medical fraud, and other harms. The personal content shared with third parties allows personal content to be aggregated with other data to identify and target Plaintiffs and the Illinois Subclass members. It is reasonable for Plaintiffs and the Illinois Subclass members to obtain identity protection or credit monitoring services in light of the foregoing. Plaintiffs and the Illinois Subclass members seek to recover the cost of these services from Facebook.

666. Facebook invaded Plaintiffs' and the Illinois Subclass members' privacy by failing to keep them informed about the nature of the app developers' business, or the purposes for which app developers were obtaining their personal content. Facebook did not disclose the nature or the extent of the exploitation of Plaintiffs' and the Illinois Subclass members' personal content. Facebook invaded Plaintiffs' and the Illinois Subclass members' privacy by subjecting them to psychographic marketing that exploited intimate aspects of their identity, including emotional and psychological manipulation.

667. Plaintiffs' and the Illinois Subclass members' personal content was exploited without informed consent. Accordingly, Plaintiffs and the Illinois Subclass members are entitled to part of Facebook's profits that were generated by their personal content without informed consent.

668. Plaintiffs and the Illinois Subclass members seek all monetary and non-monetary relief allowed by law, including damages, restitution, punitive damages, injunctive relief, and reasonable attorneys' fees and costs.

**Claim XVI. Violations of the Iowa Private Right of Action for Consumer Frauds Act  
Iowa Code Ann. § 714H  
(Against Facebook) (In the Alternative)**

669. The Iowa Plaintiff identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Iowa Subclass, incorporates by reference all allegations of this complaint as though fully set forth herein.

670. Facebook is a "person" as defined by Iowa Code Ann. § 714H.2(7).

671. Plaintiff and the Iowa Subclass members are "consumer[s]" as defined by Iowa Code § 714H.2(3).

672. Facebook's conduct described herein related to or was in connection with the "sale" or "advertisement" of "merchandise" as defined by Iowa Code Ann. § 714H.2(2), (6), (8).

673. Facebook engaged in unfair, deceptive, and unconscionable trade practices, in violation of the Iowa Private Right of Action for Consumer Frauds Act, as described throughout and herein.

674. Facebook's representations and omissions were material because they were likely to deceive reasonable consumers to believe their user data could be and was kept private.

675. Facebook intended to mislead Plaintiff and the Iowa Subclass members and induce them to rely on its misrepresentations and omissions.

676. Facebook acted intentionally, knowingly, and maliciously to violate Iowa's Private Right of Action for Consumer Frauds Act, and recklessly disregarded Plaintiff and the Iowa Subclass members' rights.

677. As a direct and proximate result of Facebook's unfair and deceptive acts and practices, Plaintiff and Iowa Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in using Facebook's services.

678. Plaintiff and the Iowa Subclass members have suffered injuries in fact and lost money or property due to Defendant's business acts or practices. Plaintiff's and the Iowa Subclass members' personal content has tangible value. Their personal content is in the possession of third parties who have used and will use it for their own advantage, including financial advantage, or was and is being sold for value, making it clear that the personal content has tangible value.

679. Plaintiff and the Iowa Subclass members are at increased risk of identity theft due to Facebook's practices concerning sharing data with third parties. Plaintiff and the Iowa Subclass members may be subjected to voter fraud, identity theft, medical fraud, and other harms. The personal content shared with third parties allows personal content to be aggregated with other data to identify and target Plaintiff and Iowa Subclass members. It is reasonable for Plaintiff and the Iowa Subclass members to obtain identity protection or credit monitoring services in light of the foregoing. Plaintiff and Iowa Subclass members seek to recover the cost of these services from Facebook.

680. Facebook invaded Plaintiff's and the Iowa Subclass members' privacy by failing to keep them informed about the nature of the app developers' business, or the purposes for



which app developers were obtaining their personal content. Facebook did not disclose the nature or the extent of the exploitation of Plaintiff's and the Iowa Subclass members' personal content. Facebook invaded Plaintiff's and the Iowa Subclass members' privacy by subjecting them to psychographic marketing that exploited intimate aspects of their identity, including emotional and psychological manipulation.

681. Plaintiff's and the Iowa Subclass members' personal content was exploited without informed consent. Accordingly, Plaintiff and the Iowa Subclass members are entitled to part of Facebook's profits that were generated by their personal content without informed consent.

682. Plaintiff has provided notice to the Iowa Attorney General and has received the Attorney General's approval pursuant to Iowa Code Ann. § 714H.7.

683. Plaintiff and Iowa Subclass members seek all monetary and non-monetary relief allowed by law, including injunctive relief, damages, punitive damages, and reasonable attorneys' fees and costs.

**Claim XVII. Violations of the Kansas Consumer Protection Act**  
**Kan. Stat. Ann. §§ 50-623 *et seq.***  
**(Against Facebook) (In the Alternative)**

684. The Kansas Plaintiff identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Kansas Subclass, incorporates by reference all allegations of this complaint as though fully set forth herein.

685. Kan. Stat. Ann. §§ 50-623 *et seq.* is to be liberally construed to protect consumers from suppliers who commit deceptive and unconscionable practices.

686. Plaintiff and the Kansas Subclass members are "consumer[s]" as defined by Kan. Stat. Ann. § 50-624(b).

687. The acts and practices described herein are "consumer transaction[s]," as defined by Kan. Stat. Ann. § 50-624(c).

688. Facebook is a "supplier" as defined by Kan. Stat. Ann. § 50-624(l).

689. Facebook advertised, offered, or sold goods or services in Kansas and engaged in

trade or commerce directly or indirectly affecting the people of Kansas.

690. Facebook's representations and omissions were material because they were likely to deceive reasonable consumers to believe their user data could be and was kept private.

691. Facebook intended to mislead Plaintiff and the Kansas Subclass members and induce them to rely on its misrepresentations and omissions.

692. Had Facebook disclosed to Plaintiff and the Kansas Subclass members that it misrepresented and omitted material information about the nature of the privacy of user data, users' ability to control how their data was used, and access of user data to third parties, and was otherwise engaged in deceptive, common business practices, Facebook would have been unable to continue in business and it would have been forced to disclose the defects in its privacy protection. Instead, Facebook represented that its services were protecting user privacy and that users could control the use of the private data. Plaintiff and the Kansas Subclass members acted reasonably in relying on Facebook's misrepresentations and omissions, the truth of which they could not have discovered.

693. Facebook also engaged in unconscionable acts and practices in connection with a consumer transaction, in violation of Kan. Stat. Ann. § 50-627, including: knowingly taking advantage of the inability of Plaintiff and the Kansas Subclass to reasonably protect their privacy interests, due to their lack of knowledge (*see id.* § 50-627(b)(1)); and requiring Plaintiff and the Kansas Subclass to enter into a consumer transaction on terms that Facebook knew were substantially one-sided in favor of Facebook particularly as concerned users' private data (*see id.* § 50-627(b)(5)).

694. Plaintiff and the Kansas Subclass members had unequal bargaining power with respect to their use of Facebook's services because of Facebook's omissions and misrepresentations.

695. The above unfair, deceptive, and unconscionable practices and acts by Facebook were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and the Kansas Subclass members that they could not reasonably avoid; this substantial

injury outweighed any benefits to consumers or to competition.

696. Facebook acted intentionally, knowingly, and maliciously to violate Kansas's Consumer Protection Act, and recklessly disregarded Plaintiff and the Kansas Subclass members' rights.

697. As a direct and proximate result of Facebook's unfair, deceptive, and unconscionable trade practices, Plaintiff and the Kansas Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in using Facebook's services.

698. Plaintiff and the Kansas Subclass members have suffered injuries in fact and lost money or property due to Defendant's business acts or practices. Plaintiff's and the Kansas Subclass members' personal content has tangible value. Their personal content is in the possession of third parties who have used and will use it for their own advantage, including financial advantage, or was and is being sold for value, making it clear that the personal content has tangible value.

699. Plaintiff and the Kansas Subclass members are at increased risk of identity theft due to Facebook's practices concerning sharing data with third parties. Plaintiff and the Kansas Subclass members may be subjected to voter fraud, identity theft, medical fraud, and other harms. The personal content shared with third parties allows personal content to be aggregated with other data to identify and target Plaintiff and the Kansas Subclass members. It is reasonable for Plaintiff and the Kansas Subclass members to obtain identity protection or credit monitoring services in light of the foregoing. Plaintiff and the Kansas Subclass members seek to recover the cost of these services from Facebook.

700. Facebook invaded Plaintiff's and the Kansas Subclass members' privacy by failing to keep them informed about the nature of the app developers' business, or the purposes for which app developers were obtaining their personal content. Facebook did not disclose the nature or the extent of the exploitation of Plaintiff's and the Kansas Subclass members' personal

content. Facebook invaded Plaintiff's and the Kansas Subclass members' privacy by subjecting them to psychographic marketing that exploited intimate aspects of their identity, including emotional and psychological manipulation.

701. Plaintiff's and the Kansas Subclass members' personal content was exploited without informed consent. Accordingly, Plaintiff and the Kansas Subclass members are entitled to part of Facebook's profits that were generated by their personal content without informed consent.

702. Plaintiff and the Kansas Subclass members seek all monetary and non-monetary relief allowed by law, including civil penalties or actual damages (whichever is greater), under Kan. Stat. Ann. §§ 50-634, 50-636; injunctive relief; and reasonable attorneys' fees and costs.

**Claim XVIII. Violations of the Michigan Consumer Protection Act  
Mich. Comp. Laws Ann. §§ 445.901 *et seq.*  
(Against Facebook) (In the Alternative)**

703. The Michigan Plaintiff identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Michigan Subclass, incorporates by reference all allegations of this complaint as though fully set forth herein.

704. Facebook and Michigan Subclass members are "person[s]" as defined by Mich. Comp. Laws Ann. § 445.902(1)(d).

705. Facebook advertised, offered, or sold goods or services in Michigan and engaged in trade or commerce directly or indirectly affecting the people of Michigan, as defined by Mich. Comp. Laws Ann. § 445.902(1)(g).

706. Facebook engaged in unfair, unconscionable, and deceptive practices in the conduct of trade and commerce, in violation of Mich. Comp. Laws Ann. § 445.903(1), including:

- a. "Making a representation of fact or statement of fact material to the transaction such that a person reasonably believes the represented or suggested state of affairs to be other than it actually is." *Id.* § 445.903(1)(bb); and

- b. “Failing to reveal facts that are material to the transaction in light of representations of fact made in a positive manner.” *Id.* § 445.903(1)(cc).

707. Facebook’s representations and omissions were material because they were likely to deceive reasonable consumers to believe their user data could be and was kept private.

708. Facebook intended to mislead Plaintiff and the Michigan Subclass members and induce them to rely on its misrepresentations and omissions.

709. Facebook acted intentionally, knowingly, and maliciously to violate Michigan’s Consumer Protection Act, and recklessly disregarded Plaintiff and the Michigan Subclass members’ rights.

710. As a direct and proximate result of Facebook’s unfair, deceptive, and unconscionable trade practices, Plaintiff and the Michigan Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in using Facebook’s services.

711. Plaintiff and the Michigan Subclass members have suffered injuries in fact and lost money or property due to Defendant’s business acts or practices. Plaintiff’s and the Michigan Subclass members’ personal content has tangible value. Their personal content is in the possession of third parties who have used and will use it for their own advantage, including financial advantage, or was and is being sold for value, making it clear that the personal content has tangible value.

712. Plaintiff and the Michigan Subclass members are at increased risk of identity theft due to Facebook’s practices concerning sharing data with third parties. Plaintiff and the Michigan Subclass members may be subjected to voter fraud, identity theft, medical fraud, and other harms. The personal content shared with third parties allows personal content to be aggregated with other data to identify and target Plaintiff and the Michigan Subclass members. It is reasonable for Plaintiff and the Michigan Subclass members to obtain identity protection or credit monitoring services in light of the foregoing. Plaintiff and Michigan Subclass members

seek to recover the cost of these services from Facebook.

713. Facebook invaded Plaintiff's and the Michigan Subclass members' privacy by failing to keep them informed about the nature of the app developers' business, or the purposes for which app developers were obtaining their personal content. Facebook did not disclose the nature or the extent of the exploitation of Plaintiff's and the Michigan Subclass members' personal content. Facebook invaded Plaintiff's and the Michigan Subclass members' privacy by subjecting them to psychographic marketing that exploited intimate aspects of their identity, including emotional and psychological manipulation.

714. Plaintiff's and the Michigan Subclass members' personal content was exploited without informed consent. Accordingly, Plaintiff and the Michigan Subclass members are entitled to part of Facebook's profits that were generated by their personal content without informed consent.

715. Plaintiff and the Michigan Subclass members seek all monetary and non-monetary relief allowed by law, including the greater of actual damages or \$250, injunctive relief, and any other relief that is just and proper.

**Claim XIX. Violations of the New York General Business Law  
N.Y. Gen. Bus. Law §§ 349 *et seq.*  
(Against Facebook) (In the Alternative)**

716. The New York Plaintiff identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the New York Subclass, incorporates by reference all allegations of this complaint as though fully set forth herein.

717. Facebook engaged in deceptive acts or practices in the conduct of its business, trade, and commerce or furnishing of goods or services, in violation of N.Y. Gen. Bus. Law § 349, as described herein.

718. Facebook's representations and omissions were material because they were likely to deceive reasonable consumers to believe their user data could be and was kept private.

719. Facebook acted intentionally, knowingly, and maliciously to violate New York's General Business Law, and recklessly disregarded Plaintiff and the New York Subclass

members' rights.

720. As a direct and proximate result of Facebook's unfair, deceptive, and unconscionable trade practices, Plaintiff and the New York Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in using Facebook's services and keeping their data private.

721. Facebook's deceptive and unlawful acts and practices complained of herein affected the public interest and consumers at large, including the millions of New Yorkers who use Facebook's services.

722. The above deceptive and unlawful practices and acts by Facebook caused substantial injury to Plaintiff and New York Subclass members that they could not reasonably avoid.

723. As a direct and proximate result of Facebook's unfair and deceptive acts and practices, Plaintiff and the New York Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in using Facebook's services.

724. Plaintiff and the New York Subclass members have suffered injuries in fact and lost money or property due to Defendant's business acts or practices. Plaintiff's and the New York Subclass members' personal content has tangible value. Their personal content is in the possession of third parties who have used and will use it for their own advantage, including financial advantage, or was and is being sold for value, making it clear that the personal content has tangible value.

725. Plaintiff and the New York Subclass members are at increased risk of identity theft due to Facebook's practices concerning sharing data with third parties. Plaintiff and the New York Subclass members may be subjected to voter fraud, identity theft, medical fraud, and other harms. The personal content shared with third parties allows personal content to be aggregated with other data to identify and target Plaintiff and the New York Subclass members.



It is reasonable for Plaintiff and the New York Subclass members to obtain identity protection or credit monitoring services in light of the foregoing. Plaintiff and the New York Subclass members seek to recover the cost of these services from Facebook.

726. Facebook invaded Plaintiff's and the New York Subclass members' privacy by failing to keep them informed about the nature of the app developers' business, or the purposes for which app developers were obtaining their personal content. Facebook did not disclose the nature or the extent of the exploitation of Plaintiff's and the New York Subclass members' personal content. Facebook invaded Plaintiff's and the New York Subclass members' privacy by subjecting them to psychographic marketing that exploited intimate aspects of their identity, including emotional and psychological manipulation.

727. Plaintiff's and the New York Subclass members' personal content was exploited without informed consent. Accordingly, Plaintiff and the New York Subclass members are entitled to part of Facebook's profits that were generated by their personal content without informed consent.

728. Plaintiff and New York Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages of \$50 (whichever is greater), treble damages, injunctive relief, and attorney's fees and costs.

**Claim XX. Violations of the Washington Consumer Protection Act  
Wash. Rev. Code Ann. §§ 19.86.010 *et seq.*  
(Against Facebook) (In the Alternative)**

729. The Washington Plaintiffs identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Washington Subclass, incorporates by reference all allegations of this complaint as though fully set forth herein.

730. Facebook is a "[p]erson," as defined by Wash. Rev. Code Ann. § 19.86.010(1).

731. Facebook advertised, offered, or sold goods or services in Washington and engaged in trade or commerce directly or indirectly affecting the people of Washington, as defined by Wash. Rev. Code Ann. § 19.86.010(2).

732. Facebook engaged in unfair or deceptive acts or practices in the conduct of trade

or commerce, in violation of Wash. Rev. Code Ann. § 19.86.020, as described herein.

733. Facebook's representations and omissions were material because they were likely to deceive reasonable consumers to believe their user data could be and was kept private.

734. Facebook acted intentionally, knowingly, and maliciously to violate Washington's Consumer Protection Act, and recklessly disregarded Plaintiff and Washington Subclass members' rights. Facebook's knowledge of the improper protection and use of private user data, and release of private user data, put it on notice that the services were not as it advertised.

735. Facebook's conduct is injurious to the public interest because it violates Wash. Rev. Code Ann. § 19.86.020, violates a statute that contains a specific legislation declaration of public interest impact, and/or injured persons and had and has the capacity to injure persons. Further, its conduct affected the public interest, including the at least hundreds of thousands of Washingtonians affected by Facebook's deceptive business practices.

736. As a direct and proximate result of Facebook's unfair methods of competition and unfair or deceptive acts or practices, Plaintiff and the Washington Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in using Facebook's services.

737. Plaintiff and the Washington Subclass members have suffered injuries in fact and lost money or property due to Defendant's business acts or practices. Plaintiff's and the Washington Subclass members' personal content has tangible value. Their personal content is in the possession of third parties who have used and will use it for their own advantage, including financial advantage, or was and is being sold for value, making it clear that the personal content has tangible value.

738. Plaintiff and the Washington Subclass members are at increased risk of identity theft due to Facebook's practices concerning sharing data with third parties. Plaintiff and the Washington Subclass members may be subjected to voter fraud, identity theft, medical fraud, and other harms. The personal content shared with third parties allows personal content to be

aggregated with other data to identify and target Plaintiff and the Washington Subclass members. It is reasonable for Plaintiff and the Washington Subclass members to obtain identity protection or credit monitoring services in light of the foregoing. Plaintiff and the Washington Subclass members seek to recover the cost of these services from Facebook.

739. Facebook invaded Plaintiff's and the Washington Subclass members' privacy by failing to keep them informed about the nature of the app developers' business, or the purposes for which app developers were obtaining their personal content. Facebook did not disclose the nature or the extent of the exploitation of Plaintiff's and the Washington Subclass members' personal content. Facebook invaded Plaintiff's and the Washington Subclass members' privacy by subjecting them to psychographic marketing that exploited intimate aspects of their identity, including emotional and psychological manipulation.

740. Plaintiff's and the Washington Subclass members' personal content was exploited without informed consent. Accordingly, Plaintiff and the Washington Subclass members are entitled to part of Facebook's profits that were generated by their personal content without informed consent.

741. Plaintiff and the Washington Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages, treble damages, injunctive relief, civil penalties, and attorneys' fees and costs.

**Claim XXI. Violations of the West Virginia Consumer Credit and Protection Act  
(Against Facebook) (In the Alternative)  
W. Va. Code ann. §§ 46A-6-101 *et seq.***

742. The West Virginia Plaintiff identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the West Virginia Subclass, incorporates by reference all allegations of this complaint as though fully set forth herein.

743. Plaintiff and West Virginia Subclass members are "[c]onsumer[s]," as defined by W. Va. Code Ann. § 46A-6-102(2).

744. Facebook engaged in "consumer transaction[s]," as defined by W. Va. Code Ann. § 46A-6-102(2).

745. Facebook advertised, offered, or sold goods or services in West Virginia and engaged in trade or commerce directly or indirectly affecting the people of West Virginia, as defined by W. Va. Code Ann. § 46A-6-102(6).

746. Facebook has been on notice concerning its wrongful conduct as alleged herein by Plaintiff and the West Virginia Subclass members. However, sending pre-suit notice pursuant to W. Va. Code § 46A-6-106(c) is an exercise in futility for Plaintiff, because, despite being on knowledge of the deceptive acts and practices complained of herein in this lawsuit as of the date of the first-filed lawsuit in March 2018, Facebook has not cured its unfair and deceptive acts and practices.

747. Facebook engaged in unfair and deceptive business acts and practices in the conduct of trade or commerce, in violation of W. Va. Code Ann. § 46A-6-104, as described herein.

748. Facebook's unfair and deceptive acts and practices also violated W. Va. Code Ann. § 46A-6-102(7), including:

- a. "Engaging in any other conduct which similarly creates a likelihood of confusion or of misunderstanding." *Id.* § 46A-6-102(7)(L); and
- b. "The act, use or employment by any person of any deception, fraud, false pretense, false promise or misrepresentation, or the concealment, suppression or omission of any material fact with intent that others rely upon such concealment, suppression or omission, in connection with the sale or advertisement of any goods or services, whether or not any person has in fact been misled, deceived or damaged thereby." *Id.* § 46A-6-102(7)(M).

749. Facebook's unfair and deceptive acts and practices were unreasonable when weighed against the need to develop or preserve business, and were injurious to the public interest, under W. Va. Code Ann. § 46A-6-101.

750. Facebook's acts and practices were additionally "[u]nfair" under W. Va. Code

Ann. § 46A-6-104 because they caused or were likely to cause substantial injury to consumers which was not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.

751. The injury to consumers from Facebook's conduct was and is substantial because it was non-trivial and non-speculative; and involved an ascertainable injury. The injury to consumers was substantial not only because it inflicted harm on a significant and unprecedented number of consumers, but also because it inflicted a significant amount of harm on each consumer.

752. Consumers could not have reasonably avoided injury because Facebook's business acts and practices unreasonably created or took advantage of an obstacle to the free exercise of consumer decision-making. By withholding important information from consumers, Facebook created an asymmetry of information between it and consumers that precluded consumers from taking action to avoid or mitigate injury.

753. Facebook's business practices had no countervailing benefit to consumers or to competition.

754. Facebook's acts and practices were additionally "deceptive" under W. Va. Code Ann. § 46A-6-104 because Facebook made representations or omissions of material facts that misled or were likely to mislead reasonable consumers, including Plaintiff and West Virginia Subclass members.

755. Facebook intended to mislead Plaintiff and the West Virginia Subclass members and induce them to rely on its misrepresentations and omissions.

756. Facebook's representations and omissions were material because they were likely to deceive reasonable consumers to believe their user data could be and was kept private.

757. Had Facebook disclosed to Plaintiff and the West Virginia Subclass members that it misrepresented and omitted material information about the nature of the privacy of user data, users' ability to control how their data was used, and access of user data to third parties, and was otherwise engaged in deceptive, common business practices, Facebook would have been unable

to continue in business and it would have been forced to disclose the defects in its privacy protection. Instead, Facebook represented that its services were protecting user privacy and that users could control the use of the private data. Plaintiff and the West Virginia Subclass members acted reasonably in relying on Facebook's misrepresentations and omissions, the truth of which they could not have discovered.

758. Facebook had a duty to disclose the above-described facts due to the circumstances of this case. Facebook's duty to disclose arose from its:

- a. Possession of exclusive knowledge regarding the defects in its services;
- b. Possession of exclusive knowledge regarding its services and inadequate protection and abuse of user data;
- c. Active concealment of the defects in its services and protection and abuse of user data; and
- d. Incomplete representations about its services and protection and abuse of user data.

759. Facebook's omissions were legally presumed to be equivalent to active misrepresentations because Facebook intentionally prevented Plaintiff and the West Virginia Subclass members from discovering the truth regarding Facebook's use, sale, disclosure and abuse of private user data.

760. Facebook acted intentionally, knowingly, and maliciously to violate West Virginia's Consumer Credit and Protection Act, and recklessly disregarded Plaintiff and the West Virginia Subclass members' rights.

761. As a direct and proximate result of Facebook's unfair and deceptive acts or practices and Plaintiff and the West Virginia Subclass members' purchase of goods or services, Plaintiff and West Virginia Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from not receiving the benefit of their bargain in using Facebook's services.

762. Plaintiff and the West Virginia Subclass members have suffered injuries in fact

and lost money or property due to Defendant's business acts or practices. Plaintiff's and the West Virginia Subclass members' personal content has tangible value. Their personal content is in the possession of third parties who have used and will use it for their own advantage, including financial advantage, or was and is being sold for value, making it clear that the personal content has tangible value.

763. Plaintiff and the West Virginia Subclass members are at increased risk of identity theft due to Facebook's practices concerning sharing data with third parties. Plaintiff and the West Virginia Subclass members may be subjected to voter fraud, identity theft, medical fraud, and other harms. The personal content shared with third parties allows personal content to be aggregated with other data to identify and target Plaintiff and the West Virginia Subclass members. It is reasonable for Plaintiff and the West Virginia Subclass members to obtain identity protection or credit monitoring services in light of the foregoing. Plaintiff and the West Virginia Subclass members seek to recover the cost of these services from Facebook.

764. Facebook invaded Plaintiff's and the West Virginia Subclass members' privacy by failing to keep them informed about the nature of the app developers' business, or the purposes for which app developers were obtaining their personal content. Facebook did not disclose the nature or the extent of the exploitation of Plaintiff's and the West Virginia Subclass members' personal content. Facebook invaded Plaintiff's and the West Virginia Subclass members' privacy by subjecting them to psychographic marketing that exploited intimate aspects of their identity, including emotional and psychological manipulation.

765. Plaintiff's and the West Virginia Subclass members' personal content was exploited without informed consent. Accordingly, Plaintiff and the West Virginia Subclass members are entitled to part of Facebook's profits that were generated by their personal content without informed consent.

766. Facebook's violations present a continuing risk to Plaintiff and the West Virginia Subclass members as well as to the general public.

767. Plaintiff and the West Virginia Subclass members seek all monetary and non-



monetary relief allowed by law, including the greater of actual damages or \$200 per violation under W. Va. Code Ann. § 46A-6-106(a), restitution, injunctive and other equitable relief, punitive damages, and reasonable attorneys' fees and costs.

**C. Non-Prioritized Claims**

**Claim XXII. Racketeer Influence and Corrupt Organizations Act, 18 U.S.C. § 1962(c) (Against Prioritized Defendant Facebook Inc.; Doe Defendants and Non-Prioritized Defendants Kogan, Bannon, SCL Group, and GSR as “Co-Conspirators”)**

768. Plaintiffs incorporate by reference all allegations of this complaint as though fully set forth herein.

769. Plaintiffs, individually, and on behalf of the Class, assert violations of 18 U.S.C. § 1962(C).

770. Upon information and belief, the Defendants associated with GSR, Cambridge-Analytica-related-entities and other unnamed Co-Conspirator related entities, for the purpose of utilizing illicitly obtained User Information for the targeting of digital political propaganda (the “Digital Political Propaganda Enterprise”). The Defendants therefore constitute a RICO enterprise pursuant to 18 U.S.C. § 1961(4). In the alternative, these individuals and entities constitute an enterprise because they associated together for the common purpose of utilizing illicitly obtained personally identifiable information for the targeting of digital political propaganda.

771. Upon information and belief, the Digital Political Propaganda Enterprise is an enterprise engaged in, and whose activities affect, interstate commerce. This enterprise has been in operation since at least 2014.

772. The association-in-fact Digital Political Propaganda Enterprise consisted of the following structure: the Co-Conspirator Defendants—Aleksandr Kogan and Stephen K. Bannon—along with Non-Defendant Co-Conspirators Cambridge Analytica and other related entities, and yet unknown third parties involved in data mining and data analysis, operated an association-in-fact enterprise, which was formed for the purpose of utilizing illicitly obtained User Information for the targeting of digital political propaganda. Each of the Co-Conspirator

Defendants was employed by or associated with, and conducted or participated in the affairs of the Digital Political Propaganda Enterprise:

A. Aleksandr Kogan participated in, operated and/or directed the Digital Political Propaganda Enterprise by, among other things: (i) creating a U.K. company called Global Science Research, Ltd. (“GSR”) which was part of a scheme to dupe users into providing their User Information, which was part of the broader scheme of illegally harvesting of data; (ii) through GSR, creating a Facebook app called “ThisIsYourDigitalLife” (“YDL”) which consisted of a personality quiz; (iii) utilizing Amazon Mechanical Turk’s (“MTurk”) program to recruit participants (known as “Turkers”) to complete the personality quiz; and (iv) utilizing the data gathered through the quiz to improperly harvest the data of millions of Facebook subscribers;

B. Stephen K. Bannon participated in, operated and/or directed the Digital Political Propaganda Enterprise by, among other things: (i) founded Cambridge Analytica; (ii) obtained funding for the efforts of Cambridge Analytica; (iii) acted as a Vice-President of Cambridge Analytica and (iv) oversaw the efforts of Cambridge Analytica to collect troves of Facebook data.

773. The actions of the Co-Conspirator Defendants were undertaken with fraud, malice, or oppression, or with a willful and conscious disregard of the rights or safety of Plaintiffs and class members. As such, Plaintiffs and each of the Class members are entitled to an award of exemplary and punitive damages against each of the Co-Conspirator Defendants in an amount according to proof at trial.

774. The Co-Conspirator Defendants worked together to accomplish their scheme or common course of conduct. This enterprise has been in operation since at least 2014.

775. The racketeering activity committed by each of the members of the Digital Political Propaganda Enterprise affected interstate commerce.

776. On information and belief, the Co-Conspirator Defendants agreed to and did conduct and participate, directly and indirectly, in the conduct of the Digital Political Propaganda

Enterprise's affairs in a pattern of racketeering activity targeted at intentionally defrauding Facebook users including, without limitation, via nominal payments and numerous intentionally false representations averred herein with the specific intent of inducing Facebook users to unwittingly share other users' private User Information.

777. Pursuant to and in furtherance of their corrupt scheme, the Co-Conspirator Defendants did in fact induce Facebook users to share other Facebook users' User Information via hundreds of thousands of separate electronic monetary transfers.

778. The Co-Conspirator Defendants willfully and knowingly devised a scheme with artifice to defraud Facebook users and to obtain, sell, and use personal User Information by false pretenses and representations, including, but not limited to, the representation that the data would only be used for academic purposes.

779. The payments made or directed by the Co-Conspirator Defendants or any other entity to obtain Facebook data compromised in the Your DigitalLife scandal were in furtherance of the fraudulent scheme. On information and belief, those payments were made by wire transfer or other electronic means through interstate or foreign commerce.

780. The payments made from any of the Co-Conspirator Defendants or directed by any Co-Conspirator to takers of the Your DigitalLife quiz were in furtherance of the fraudulent scheme. On information and belief, those payments were made by wire transfer or other electronic means through interstate or foreign commerce.

781. The acts of wire fraud averred herein constitute a pattern of racketeering activity pursuant to 18 U.S.C. § 1961(5).

782. The Co-Conspirator Defendants have directly and indirectly participated in the conduct of the Conspiracy's affairs through the pattern of racketeering and activity alleged herein, in violation of 18 U.S.C. § 1962(c). Facebook aided and abetted the Co-Conspirator Defendants by misleading its users to believe that their data was safe, while permitting third-party apps like GSR's to access and use the data of non-consenting users without their permission and knowledge, and the other Co-Conspirator Defendants directly participated in the

conspiracy by misleading quiz-takers that they were allowing Co-Conspirator Defendants' access to only their personal data for academic purposes, when in fact they were allowing access to their friends' data, and by fraudulently obtaining the data, selling it in interstate and foreign commerce, and using it to influence elections.

783. Plaintiffs and Class members were harmed by the Co-Conspirator Defendants' conduct because the private information they did not intend to become public or disclose to third parties was acquired by companies who intended to and did use it illicitly for manipulating elections and other as yet unknown purposes. Furthermore, the security breach put Plaintiffs and Class members in imminent and real danger of having their identities stolen by anyone willing to pay these unscrupulous companies for the data. In addition, Plaintiffs and class members spent time and money securing their personal information and protecting their identities, by, for instance, purchasing identity theft protection.

784. As a direct and proximate result of the Co-Conspirator Defendants' racketeering activities and violations of 18 U.S.C. § 1962(c), Plaintiffs and the Class have been injured.

785. Plaintiffs demand judgment in their favor and against the Co-Conspirator Defendants jointly and severally for compensatory, treble, and punitive damages with interest, the costs of suit and attorneys' fees, and other and further relief as this Court deems just and proper.

**Claim XXIII. Misappropriation of Valuable Property  
(Against Prioritized Defendant Facebook Inc.; Doe Defendants;)**

786. Plaintiffs incorporate by reference all allegations of this complaint as though fully set forth herein.

787. Defendants' actions constitute misappropriation.

788. Defendants used Plaintiffs' and Class members' valuable personal and private information in violation of Facebook's promises to protect their privacy.

789. Plaintiffs and Class members did not consent to this use.

790. Defendants' gained a commercial benefit by using Plaintiffs' and Class members' valuable personal and private information when Defendant misappropriated, used, and/or sold

for profit Plaintiffs' and Class members' valuable personal and private information.

791. Plaintiffs and members of the Class were harmed.

792. Defendants' conduct was a substantial factor in causing Plaintiffs' and Class members' harm.

793. Accordingly, Plaintiffs and members of the Classes are entitled to relief.

**Claim XXIV. Fraudulent Misrepresentation  
(Against Prioritized Defendant Facebook Inc.)**

794. Plaintiffs incorporate by reference all allegations of this complaint as though fully set forth herein.

795. Plaintiffs and members of the Nationwide Class are entitled to a measure of damages for common law fraud under the California Civil Code for the fraud described herein.

796. Defendant Facebook stored the personal information of Plaintiffs and members of the Class in its electronic and consumer information databases. Defendant falsely and knowingly represented to Plaintiffs and members of the Class that their personal information would remain private. Defendant fraudulently represented that it would not disclose this personal information without authorization, and/or by obtaining that personal information without authorization.

797. Defendant Facebook's statements that it would maintain the confidentiality of Plaintiffs' and the Class's personal information was false because Defendant knowingly and intentionally provided that information to GSR. GSR then passed this information to Cambridge Analytica which used it for its own advantage or for commercial profit, without either any permission or sufficient permission from the users. Defendant Facebook knew that it did not have users' permission to disclose personal information to third parties because Defendant did not attempt in any way to obtain permission from the up to 87 million users whose personal information was disclosed to Cambridge Analytica.

798. Plaintiffs and the Class members suffered injury in fact and lost money or property as the proximate result of Defendant's fraudulent misrepresentation. In particular, the personal information of Plaintiffs and Class members was taken and is in the hands of those who will and did use it for their own advantage, or was and is being sold for value, making it clear

that the stolen information has tangible value.

799. Plaintiffs and the Class justifiably relied on the representations Defendant Facebook made in its publicly available privacy policy and elsewhere that it would not “share information we receive about you with others unless we have: received your permission [and] given you notice.”

800. As described with specificity above, Defendant knew the falsity of its representations, and they were made with the intent to deceive Plaintiffs and members of the Class into supplying Facebook with private confidential personal information. Facebook’s representations regarding the maintenance of user confidentiality and privacy were material to Plaintiffs’ and Class members’ decision to provide Facebook with the personal information Facebook subsequently disclosed to Cambridge Analytica. Plaintiffs and members of the Class justifiably relied upon the representations of Defendant.

801. Plaintiffs and members of the Class suffered harm as a proximate result of Defendant’s fraudulent acts.

802. As a result of Defendant’s fraudulent misrepresentations, Plaintiffs and the Class are entitled to general damages, special damages in an amount according to proof, punitive damages, reasonable attorneys’ fees and costs, and any other relief that the Court deems proper or available for common law fraud, and injunctive relief.

**Claim XXV. Negligent Misrepresentation  
(Against Prioritized Defendant Facebook Inc.)**

803. Plaintiffs incorporate by reference all allegations of this complaint as though fully set forth herein.

804. As alleged herein, Defendant Facebook, through its agent and Chief Executive Officer, Mark Zuckerberg, repeatedly assured Plaintiffs and Class Members that their data would be private and protected.

805. Defendant Facebook further assured that users’ data would not be shared with third-party applications without users’ express permission.

806. At the time Defendant Facebook made these representations, Defendant knew or

should have known that these representations were false or made them without knowledge of their truth or veracity.

807. At minimum, Defendant Facebook negligently misrepresented and/or negligently omitted material facts concerning its commitment to privacy and the safety of user data.

808. The negligent misrepresentations and omissions made by Defendant, upon which Plaintiffs and all Class members reasonably and justifiably relied, were intended to induce reliance.

**Claim XXVI. Trespass to Personal Property  
(Against Prioritized Defendant Facebook Inc.)**

809. Plaintiffs adopt and incorporate all the allegations of this complaint as if stated fully herein.

810. Defendant Facebook has repeatedly represented to Plaintiffs, as well as Class members, Congress, and other governmental bodies of the world, that users (including Plaintiffs and the Class members) “own all of the content and information [they] post on Facebook.”

811. Defendant Facebook, intentionally and without consent, or exceeding any consent previously obtained from users, shared Plaintiffs’ and Class members’ property, including their user data and Personal Information, with device manufacturers.

812. Defendant Facebook’s intentional and unauthorized, or exceeding any authorization previously obtained, sharing of Plaintiffs’ and Class members’ property, including their user data and Personal Information, interfered with Plaintiffs’ and Class members’ possessory interests in that property.

813. Defendant Facebook’s conduct caused Plaintiffs and Class members damage when the property, including user data and including Personal Information, was shared with the device manufacturers, as well as when Facebook unjustly profited from the sharing of Plaintiffs’ and Class members’ property, including user data and Personal Information, which deprived Plaintiffs and Class members of any income or other form of compensation Facebook generated through its unauthorized (or exceeding any authorization previously obtained) data-sharing partnerships.



**Claim XXVII. Conversion**  
**(Against Prioritized Defendant Facebook and Doe Defendants, and Non-Prioritized Defendants Zuckerberg, Mercer, Bannon and Kogan)**

814. Plaintiffs adopt and incorporate all the allegations of this complaint as if stated fully herein.

815. Plaintiffs and Class members were the owners and possessors of their private information. As the result of Defendants' wrongful conduct, Defendants have interfered with the Plaintiffs' and Class members' rights to possess and control such property, to which they had a superior right of possession and control at the time of conversion.

816. As a direct and proximate result of Defendants' conduct, Plaintiffs and the Class members suffered injury, damage, loss or harm and therefore seek compensatory damages.

817. In converting Plaintiffs' private information, Defendants have acted with malice, oppression, and in conscious disregard of the Plaintiffs' and Class members' rights. Plaintiffs, therefore, seek an award of punitive damages on behalf of the class.

**Claim XXVIII. Unlawful Interception of Communications – 11 Del. Code § 2401**  
**(Against Prioritized Defendant Facebook Inc.; Doe Defendants; and Non-Prioritized Defendant Kogan)**

818. Plaintiffs adopt and incorporate all the allegations of this complaint as if stated fully herein.

819. By reason of the conduct alleged herein, Defendants violated Delaware's Criminal Code protecting persons from electronic surveillance and unlawful interception of communications.

820. According to Chapter 24 of the Title 11 of the Delaware Criminal Code, "Electronic communication" includes "any transfer of signs, signals, writing, images, sounds, data or intelligence of any electromagnetic, photoelectronic or photooptical system." 11 Del. Code § 2401.

821. The messages, posts, images and countless other forms of communication on Facebook users' profiles are considered electronic communications.

822. The statute defines "Electronic communication system" as "any wire, oral, electromagnetic, photooptical, or photoelectronic facilities for the transmission of wire, oral or

electronic communications and any computer facilities or related electronic equipment.” *Id.*

823. The servers Defendant Facebook uses to provide its electronic communication service which facilitate user communication are considered an “electronic communication system”.

824. Delaware prohibits the intentional interception of any wire, oral or electronic communication unless party to the communication or with prior consent by one of the parties to the communication. 11 Del. Code § 2402(a).

825. Aleksandr Kogan, through GSR, unlawfully and intentionally intercepted electronic communications without prior consent. Kogan harvested electronic communications, including messages and private discussions, of more than 87 million users and passed a portion of this information to Cambridge Analytica and related entities, without users’ permission.

826. Delaware also prohibits a person or entity providing an electronic communications service to the public from knowingly divulging to any other person or entity the contents of a communication while the communication is in electronic storage by that service. 11 Del. Code § 2422.

827. Defendant Facebook, a “person” and “electronic communication service” pursuant to Delaware Criminal Code, unlawfully and intentionally divulged the contents of Plaintiffs’ and Class members’ communications.

828. Defendant Facebook intentionally divulged the contents of Plaintiffs’ and Class members’ stored electronic communications by allowing Aleksandr Kogan, through GSR, access to their electronic communications which also contained sensitive personal information and identifiers putting Plaintiffs and Class members at risk of being harmed.

829. Section 2409 of the Delaware Criminal Code authorizes a private right of action for actual damages, punitive damages and reasonable attorneys’ fees and other litigation costs reasonably incurred to any person whose wire, oral or electronic communication is intercepted, disclosed or used in violation of this code.

830. Plaintiffs and Class members have been harmed by Defendants’ misconduct and

are entitled to actual damages, punitive damages and reasonable attorneys' fees and costs.

**Claim XXIX. Violation of California Consumer Record Act  
(Against Facebook Inc. on Behalf of the Nationwide Class)**

831. Plaintiffs adopt and incorporate all the allegations of this complaint as if stated fully herein.

832. “[T]o ensure that personal information about California residents is protected,” the California Legislature enacted California Customer Records Act. This statute states that any business that “owns or licenses personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.” Civil Code § 1798.81.5.

833. Facebook is a “business” within the meaning of Civil Code § 1798.80(a).

834. Plaintiffs and members of the class are “individual[s]” within the meaning of the Civil Code § 1798.80(d). Pursuant to Civil Code § 1798.80(e), the user information is “personal information,” which includes, but is not limited to, an individual’s name, physical characteristics or description, address, telephone number, education, employment, employment history, and medical information.

835. The breach of the personal user information of tens of millions of Facebook customers constituted a “breach of the security system” of Facebook pursuant to Civil Code § 1798.82(g).

836. By failing to implement reasonable measures to protect its customers’ personal User Information, Facebook violated Civil Code § 1798.81.5.

837. In addition, by failing to promptly notify all affected users that their personal User Information had been acquired (or was reasonably believed to have been acquired) by unauthorized persons, including by the Co-Conspirator Cambridge Analytica and Co-Conspirator Defendants, Facebook violated Civil Code § 1798.82. Facebook’s failure to timely and adequately notify users of the breach leaves Class members vulnerable to continued misuse of their personal information and prevents Class members from taking adequate steps to protect

their identities.

838. By violating Civil Code §§ 1798.81.5 and 1798.82, Facebook “may be enjoined” pursuant to Civil Code § 1798.84(e).

839. Plaintiffs further request that the Court require Facebook to (1) identify and notify all members of the Class who have not yet been informed of the breach; and (2) notify affected former and current users and employees of any future data breaches by email within 24 hours of Facebook’s discovery of a breach or possible breach and by mail within 72 hours.

840. As a result of Facebook’s violation of Civil Code §§ 1798.81.5 and 1798.82, Plaintiffs and members of the Class have and will incur economic damages relating to time and money spent remedying the breach, including, but not limited to, monitoring their online presence to ensure that their identity has not been stolen or coopted for an illicit purpose, any unauthorized charges made on financial accounts, lack of access to funds while banks issue new cards, tax fraud, as well as the costs of credit monitoring and purchasing credit reports.

841. Plaintiffs, for themselves and on behalf of the members of the Class, seek all remedies available under Civil Code § 1798.84, including, but not limited to: (a) damages suffered by members of the Class; and (b) equitable relief.

842. Plaintiffs, for themselves and on behalf of the members of the Class, also seek reasonable attorneys’ fees and costs under applicable law including California Code of Civil Procedure § 1021.5 and Federal Rule of Civil Procedure 23.

**Claim XXX. Violation of California Invasion of Privacy Act (Cal. Pen. Code § 637.7)  
(Against Prioritized Defendant Facebook Inc.; Doe Defendants)**

843. Plaintiffs incorporate by reference all allegations of this complaint as though fully set forth herein.

844. Plaintiffs allege against all Defendants violations of the California Invasion of Privacy Act (“CIPA”), specifically California Penal Code § 637.7, for the unlawful acquisition of Plaintiffs’ and Class members’ user information without their consent.

845. California Penal Code § 630 provides that “The Legislature hereby declares that advances in science and technology have led to the development of new devices and techniques

for the purpose of eavesdropping upon private communications and that the invasion of privacy resulting from the continual and increasing use of such devices and techniques has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society.”

846. Defendants’ acts in violation of the CIPA occurred in the State of California because those acts resulted from business decisions, practices, and operating policies that Facebook developed, implemented, and utilized in the State of California and which are unlawful and constitute criminal conduct in the state of Facebook’s residence and principal business operations. Further, the data acquired from Facebook by Cambridge Analytica was housed on Facebook’s servers in California and obtained therefrom. Facebook’s implementation of its business decisions, practices, and standard ongoing policies that violate CIPA—and Cambridge Analytica’s availment of those business decisions, practices, and standard ongoing policies—took place and continue to take place in the State of California. Defendants profited and continue to profit in the State of California as a result of these repeated and systemic violations of CIPA. Defendants’ unlawful conduct, which occurred in the State of California, harmed and continues to harm Plaintiffs and Class Members.

847. Among the data points harvested by Facebook and provided to the remaining Defendants (as well as all third-party developers who used the “friends permission” feature) was the location of Plaintiffs and Class members.

848. CIPA expressly prohibits the use of “an electronic tracking device to determine the location or movement of a person.” Cal. Pen. Code § 637.7(a).

849. As defined under CIPA, “‘electronic tracking device’ means any device attached to a vehicle or other movable thing that reveals its location or movement by the transmission of electronic signals.” *Id.* § 637.7(d).

850. Facebook acquired—and Cambridge Analytica exfiltrated and used—Plaintiffs’ and Class members’ location through, inter alia, location data associated with smartphones and other mobile devices running Facebook.

851. Plaintiffs and Class members did not consent to said acquisition of location information by any Defendant.

**Claim XXXI. Violation of the California Consumers Legal Remedies Act  
(Against Facebook Inc.)**

852. Plaintiffs incorporate by reference all allegations of this complaint as though fully set forth herein.

853. Plaintiffs bring this claim on behalf of themselves and the Nationwide Class.

854. Plaintiffs bring this claim individually and on behalf of the members of the Class.

855. Facebook is a “person” within the meaning of CLRA in that it is a corporation.

856. Plaintiffs and Class members are “consumers” within the meaning of CLRA in that they are individuals who seek or acquire services for personal, family, or household purposes.

857. CLRA § 1770(a)(5) prohibits “[r]epresenting that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities which they do not have or that a person has a sponsorship, approval, status, affiliation, or connection which he or she does not have.”

858. Defendant Facebook’s conduct as alleged herein violates CLRA’s ban of proscribed practices at Cal. Civ. Code § 1770(a) in that, *inter alia*, Facebook misrepresented its services by not disclosing that it shares users’ data with device makers, by representing that it was only collecting Plaintiffs’ and Class members’ “Contact List” and by failing to represent that it was collecting their call logs and text data. At the time Facebook made these misrepresentations and omissions, it was aware that it was collecting Plaintiffs’ and Class members’ data.

859. Plaintiffs and Class members suffered injuries caused by Defendant’s misrepresentations and omissions because: (a) Plaintiffs and Class members suffered an invasion of their privacy as a result of Facebook collecting their call logs and text data and/or sharing their device data without their authorization, consent or knowledge, and (b) Plaintiffs and Class members were deprived of any income Facebook generated through its unauthorized use or sale

of data.

860. Prior to the filing of this Complaint, a CLRA notice letter was sent to Defendant Facebook which complies in all respects with California Civil Code § 1782(a).

861. Plaintiffs and Class members seek equitable relief for Facebook's violation of CLRA, as permitted by statute. This includes injunctive relief to enjoin the wrongful practices alleged herein, and to take corrective action to remedy past conduct, including ending all data-sharing partnerships still in effect and having Facebook direct all device makers with Plaintiffs' and Class members' data stored on their servers to delete that data.

**Claim XXXII. Violation of California's Computer Data Access and Fraud Act  
(Against Facebook Inc.)**

862. Plaintiffs incorporate by reference all allegations of this complaint as though fully set forth herein.

863. Plaintiffs bring this claim individually and on behalf of the members of the Nationwide Class.

864. Facebook knowingly accessed and without permission used Plaintiffs' and Class members' data in order to wrongfully control or obtain property or data in violation of California Penal Code § 502(c)(1).

865. Facebook knowingly accessed and without permission took, copied, and/or used data from Plaintiffs' and Class members' computers, computer systems and/or computer network in violation of California Penal Code § 502(c)(2).

866. Facebook knowingly and without permission used or caused to be used Plaintiffs' and Class members' computer services in violation of California Penal Code § 502(c)(3).

867. Facebook knowingly and without permission accessed or caused to be accessed Plaintiffs' and Class members' computers, computer systems, and/or computer network in violation of California Penal Code § 502(c)(7).

868. Plaintiffs and Class members suffered and continue to suffer damage as a result of Facebook's violations of the California Penal Code § 502 identified above.

869. Facebook's conduct also caused irreparable and incalculable harm and injuries to



Plaintiffs and Class members in the form of invading their privacy, and, unless enjoined, will cause further irreparable and incalculable injury, for which Plaintiffs and Class members have no adequate remedy at law.

870. Facebook willfully violated California Penal Code § 502 in disregard and derogation of the rights of Plaintiffs and Class members, and Facebook's actions as alleged above were carried out with oppression, fraud and malice.

871. Pursuant to California Penal Code § 502(e), Plaintiffs and Class members are entitled to injunctive relief, compensatory damages, punitive or exemplary damages, attorneys' fees, costs and other equitable relief.

**Claim XXXIII. Violations of Common Law Right to Privacy in the Following States: Alabama; Arizona; Colorado; Florida; Georgia; Idaho; Indiana; Iowa; Kansas; Maryland; Michigan; Missouri; Ohio; Oklahoma; Pennsylvania; Tennessee; Texas; Washington; West Virginia; and Wisconsin  
(Against Prioritized Defendant Facebook Inc.)**

872. Plaintiffs individually and on behalf of the class members incorporate by reference all allegations of this complaint as though fully set forth herein.

873. Plaintiffs bring this claim on behalf of themselves and the Nationwide Class.

874. The common law in these states prohibits the use of a person's name or likeness for the defendant's advantage, commercial or otherwise, without first obtaining that person's consent, or where appropriate the consent of that person's parent or legal guardian.

875. Facebook violated this section by allowing access to Plaintiffs' and class members' likeness—including names, like history, photographs, and video—as a service to third parties. On information and belief, access to the likeness of Plaintiffs and Class members was integral to the services Facebook offered app developers like Cambridge Analytica. App developers would not have purchased services from Facebook (including advertisements) without access to this information. Indeed, the value of the services Facebook offered to app developers was derived from this information.

876. Prior to using the Plaintiffs' and class members' likeness, Facebook never obtained consent.

877. Plaintiffs and class members did not receive any compensation in return for this use

878. Plaintiffs and class members were harmed by Facebook's improper use.

879. Plaintiffs and class members seek actual damages suffered, plus any profits attributable to Facebook's use of the unauthorized use not calculated in actual damages. Plaintiffs and class members also reserve the right to punitive damages, costs, and reasonable attorney's fees as allowed under this statute.

**Claim XXXIV. Violations of Alabama Right of Publicity Statute,  
Ala. Code § 6-5-772  
(Against Prioritized Defendant Facebook Inc.)**

880. The Alabama Plaintiff identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Alabama Subclass, incorporates by reference all allegations of this complaint as though fully set forth herein.

881. Ala. Code § 6-5-772 prohibits the use of a person's indicia of identity for the purposes of advertising or selling or soliciting goods or services without that persons consent, or where appropriate the consent of that person's parent or legal guardian.

882. Under Ala. Code § 6-5-771, indicia of identity includes those attributes of a person that serve to identify that person to an ordinary, reasonable viewer or listener and includes "name, signature, photograph, image, likeness, voice" or similar attribute of that person.

883. Defendant violated this section by allowing access to Plaintiff's and the Alabama Subclass members' content and information—including names, like history, photographs, and video—as a service to third parties. On information and belief, the content and information of Plaintiff and the Alabama Subclass members was integral to the services Facebook offered app developers like Cambridge Analytica. App developers would not have purchased services from Facebook (including advertisements) without access to this content and information. Indeed, the value of the services Facebook offered to app developers was derived from this content and information. Thus, Facebook directly benefited from this use of Plaintiff's and the Alabama Subclass members' content and information.

884. Prior to using the Plaintiff's and the Alabama Subclass members' content and information, the Defendant never obtained consent from the Plaintiffs.

885. Defendant profited from the commercial use of the Plaintiff's and the Alabama Subclass members' content and information.

886. Plaintiff and the Alabama Subclass members did not receive any compensation in return for this use.

887. According to Ala. Code § 6-5-774, Plaintiff and the Alabama Subclass members seek the greater of \$5,000 per incident or the actual damages suffered, plus any profits attributable to Defendants' use of the unauthorized use not calculated in actual damages. Plaintiff and the Alabama Subclass members also reserve the right to injunctive relief, punitive damages, costs, and reasonable attorney's fees as allowed under this statute.

**Claim XXXV. Violations of Florida Unauthorized Publication Statute,  
Fla. State Code § 540.08  
(Against Prioritized Defendant Facebook Inc.)**

888. The Florida Plaintiff identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Florida Subclass, incorporates by reference all allegations of this complaint as though fully set forth herein.

889. Plaintiff and Florida Subclass members incorporate by reference all allegations of the preceding paragraphs as though fully set forth herein.

890. Fla. Code § 540.08 prohibits the use of a person's name, portrait, photograph, or likeness for commercial purposes without the express consent of that person, or where appropriate the consent of that person's parent or legal guardian.

891. Defendant Facebook violated this section by allowing access to Plaintiff's and Florida Subclass members' content and information—including names, like history, photographs, and video—as a service to third parties. On information and belief, the content and information of Plaintiff and Florida Subclass members was integral to the services Facebook offered third party app developers like Cambridge Analytica; third party app developers would not have purchased services from Facebook (including advertisements) without access to this

information. Indeed, the value of the services Facebook offered to third party app developers was derived from this information.

892. Prior to using the Plaintiff's and Florida Subclass members' content and information, the Defendant never obtained consent.

893. Defendant profited from the commercial use of the Plaintiff's and Florida Subclass members' likeness.

894. Plaintiff and Florida Subclass members did not receive any compensation in return for this use.

895. According to Fla. Code § 540.08, Plaintiff and Florida Subclass members seek the greater of \$1,000 per incident in addition to any other remedies under common law, including actual damages, punitive damages, and injunctive relief.

**Claim XXXVI. Violations of Illinois Right of Publicity Statute,  
Ill. Comp. Stat. § 1075/10  
(Against Prioritized Defendant Facebook Inc.)**

896. The Illinois Plaintiffs identified above ("Plaintiffs," for purposes of this Count), individually and on behalf of the Illinois Subclass, incorporates by reference all allegations of this complaint as though fully set forth herein.

897. Ill. Comp. Stat. § 1075/5-30 prohibits the use of an individual's likeness including their name, signature, photograph, image, likeness, or voice for or in connection with a sale of a product or services or for purposes of advertising or promoting services without written consent of that person, or where appropriate the consent of that person's parent or legal guardian.

898. Defendant Facebook violated this section by allowing access to Plaintiffs' and the Illinois Subclass members' content and information—including names, like history, photographs, and video—as a service to third parties. On information and belief, the content and information of Plaintiffs and the Illinois Subclass members was integral to the services Facebook offered third party app developers like Cambridge Analytica; third party app developers would not have purchased services from Facebook (including advertisements) without access to this information. Indeed, the value of the services Facebook offered to third party app developers was derived

from this information.

899. Prior to using the Plaintiffs' and the Illinois Subclass members' content and information, the Defendant never obtained consent from the Plaintiffs.

900. Defendant profited from the commercial use of the Plaintiffs' and the Illinois Subclass members' likeness.

901. Plaintiffs and the Illinois Subclass members did not receive any compensation in return for this use.

902. According to Ill. Comp. Stat. § 1075/40-60, Plaintiffs seek the greater of \$1,000 per incident or the actual damages suffered, plus any profits attributable to Defendants' use of the unauthorized use not calculated in actual damages. Plaintiffs also reserve the right to punitive damages, costs, and reasonable attorney's fees as allowed under this statute.

**Claim XXXVII. Violations of Indiana Rights of Publicity Code,  
Ind. Code § 32-36-1-8  
(Against Prioritized Defendant Facebook Inc.)**

903. The Indiana Plaintiff identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Indiana Subclass, incorporates by reference all allegations of this complaint as though fully set forth herein.

904. Ind. Code § 32-36-1-8 prohibits the use of a person's name, voice, signature, photograph, image, likeness, distinctive appearance, gesture, or mannerisms in connection with a product service or commercial activity without that person's consent, or where appropriate the consent of that person's parent or legal guardian.

905. Defendant Facebook violated this section by allowing access to Plaintiff's and Indiana Subclass members' content and information—including names, like history, photographs, and video—as a service to third parties. On information and belief, the content and information of Plaintiff and Indiana Subclass members was integral to the services Facebook offered third party app developers like Cambridge Analytica; third party app developers would not have purchased services from Facebook (including advertisements) without access to this information. Indeed, the value of the services Facebook offered to third party app developers was

derived from this information.

906. Prior to using the Plaintiff's and Indiana Subclass members' content and information, the Defendant never obtained consent.

907. Defendant profited from the commercial use of the Plaintiff's and Indiana Subclass members' likeness.

908. Plaintiff and Indiana Subclass members did not receive any compensation in return for this use.

909. According to Ind. Code § 32-36-1-10 to Plaintiff and Indiana Subclass members seek the greater of \$1,000 per incident or the actual damages suffered, plus any profits attributable to Defendants' use of the unauthorized use not calculated in actual damages. to Plaintiff and Indiana Subclass members' also reserve the right to injunctive relief, punitive damages, costs, and reasonable attorney's fees as allowed under this statute.

**Claim XXXVIII. Violations of New York Right to Privacy Statute,  
N.Y. Civ. Rights Law § 51  
(Against Prioritized Defendant Facebook Inc.)**

910. The New York Plaintiff identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the New York Subclass, incorporates by reference all allegations of this complaint as though fully set forth herein.

911. N.Y. Civ. Rights Law § 51 prohibits the use of a person's name, portrait, picture, or voice for advertising purposes or for the purposes of trade without first obtaining that person's consent, or where appropriate the consent of that person's parent or legal guardian.

912. Defendant Facebook violated this section by allowing access to Plaintiff's and the New York Subclass members' rights content and information—including names, like history, photographs, and video—as a service to third parties. On information and belief, the content and information of Plaintiff and the New York Subclass members was integral to the services Facebook offered third party app developers like Cambridge Analytica; third party app developers would not have purchased services from Facebook (including advertisements) without access to this information. Indeed, the value of the services Facebook offered to third

party app developers was derived from this information.

913. Prior to using the Plaintiff's and the New York Subclass members' content and information, the Defendant never obtained consent.

914. Defendant profited from the commercial use of the Plaintiff's and the New York Subclass members' likeness.

915. Plaintiff and the New York Subclass members did not receive any compensation in return for this use.

916. According to N.Y. Civ. Rights Law § 51, to Plaintiff and the New York Subclass members seek actual damages suffered, plus any profits attributable to Defendants' use of the unauthorized use not calculated in actual damages. Plaintiff and the New York Subclass members also reserve the right to equitable relief, punitive damages, costs, and reasonable attorney's fees as allowed under this statute.

**Claim XXXIX. Violations of Ohio Right of Publicity Statute,  
Ohio Code § 2741.02  
(Against Prioritized Defendant Facebook Inc.)**

917. The Ohio Plaintiff identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Ohio Subclass, incorporates by reference all allegations of this complaint as though fully set forth herein.

918. Ohio Code § 2741.02 prohibits the use of a person's name, voice, signature, photograph, image, likeness, or distinctive appearance in connection with a product, good or service with that person's written consent, or where appropriate the consent of that person's parent or legal guardian.

919. Defendant Facebook violated this section by allowing access to Plaintiff's and the Ohio Subclass members' content and information—including names, like history, photographs, and video—as a service to third parties. On information and belief, the content and information of Plaintiff and the Ohio Subclass members was integral to the services Facebook offered third party app developers like Cambridge Analytica; third party app developers would not have purchased services from Facebook (including advertisements) without access to this information.



Indeed, the value of the services Facebook offered to third party app developers was derived from this information.

920. Prior to using the Plaintiff's and the Ohio Subclass members' content and information, the Defendant never obtained consent.

921. Defendant profited from the commercial use of the Plaintiff's and the Ohio Subclass members' likeness.

922. Plaintiff and the Ohio Subclass members did not receive any compensation in return for this use.

923. According to Ohio Code § 2741.07 (a), Plaintiff and the Ohio Subclass members seek the greater of \$2,500 per incident or the actual damages suffered, plus any profits attributable to Defendants' use of the unauthorized use not calculated in actual damages. Plaintiff and the Ohio Subclass members also reserve the right to punitive damages, costs, and reasonable attorney's fees as allowed under this statute.

**Claim XL. Violations of Oklahoma Rights of Publicity Statute,  
Okl. St. § 1449  
(Against Prioritized Defendant Facebook Inc.)**

924. The Oklahoma Plaintiff identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Oklahoma Subclass, incorporates by reference all allegations of this complaint as though fully set forth herein.

925. Okl. St. § 1449 prohibits the use of a person's name, voice, signature, photograph, or likeness in connection with a product, good or service with that person's written consent, or where appropriate the consent of that person's parent or legal guardian.

926. Defendant Facebook violated this section by allowing access to Plaintiff's and the Oklahoma Subclass members' content and information—including names, like history, photographs, and video—as a service to third parties. On information and belief, the content and information of Plaintiff and the Oklahoma Subclass members was integral to the services Facebook offered third party app developers like Cambridge Analytica; third party app developers would not have purchased services from Facebook (including advertisements)

without access to this information. Indeed, the value of the services Facebook offered to third party app developers was derived from this information.

927. Prior to using the Plaintiff's and the Oklahoma Subclass members' content and information, the Defendant never obtained consent.

928. Defendant profited from the commercial use of the Plaintiff's and the Oklahoma Subclass members' likeness.

929. Plaintiff and the Oklahoma Subclass members did not receive any compensation in return for this use.

930. According to Okl. St. § 1449, Plaintiff and the Oklahoma Subclass members seek the actual damages suffered, including any profits attributable to Defendants' use of the unauthorized use. Plaintiff and the Oklahoma Subclass members also reserve the right to punitive damages, costs, and reasonable attorney's fees as allowed under this statute.

**Claim XLI. Violations of Pennsylvania Unauthorized Use Statute, 42 Pa. Stat. § 8316 (Against Prioritized Defendant Facebook Inc.)**

931. The Pennsylvania Plaintiff identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Pennsylvania Subclass, incorporates by reference all allegations of this complaint as though fully set forth herein.

932. 42 Pa. Stat. § 8316 prohibits the use of a person's name or likeness in connection the sale of a product, goods or services without first obtaining that person's written consent, or where appropriate the consent of that person's parent or legal guardian.

933. Defendant Facebook violated this section by allowing access to Plaintiff's and the Pennsylvania Subclass' content and information—including names, like history, photographs, and video—as a service to third parties. On information and belief, Plaintiff's and the Pennsylvania Subclass' content and information was integral to the services Facebook offered third party app developers like Cambridge Analytica; third party app developers would not have purchased services from Facebook (including advertisements) without access to this information. Indeed, the value of the services Facebook offered to third party app developers was derived from this information.

934. Prior to using the Plaintiff's and the Pennsylvania Subclass' content and information, the Defendant never obtained consent.

935. Defendant profited from the commercial use of the Plaintiff's and the Pennsylvania Subclass' likeness.

936. Plaintiff and the Pennsylvania Subclass did not receive any compensation in return for this use.

937. Under 42 Pa. Stat. § 8316.1, Plaintiff and the Pennsylvania Subclass seek actual damages plus any profits attributable to Defendants' use of the unauthorized use not calculated in actual damages. Plaintiff and the Pennsylvania Subclass also reserve the right to injunctive relief as allowed under this statute.

**Claim XLII. Violations of Tennessee Protection of Personal Rights Statute  
T.C.A. § 47-25-1105  
(Against Prioritized Defendant Facebook Inc.)**

938. The Tennessee Plaintiff identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Tennessee Subclass, incorporates by reference all allegations of this complaint as though fully set forth herein.

939. T. C. A. § 47-25-1105 prohibits the use of a person's name, photograph, or likeness on or in goods, merchandise, or products entered into commerce in that state without first obtaining that person's consent, or where appropriate the consent of that person's parent or legal guardian.

940. Defendant Facebook violated this section by allowing access to Plaintiff's and the Tennessee Subclass members' content and information—including names, like history, photographs, and video—as a service to third parties. On information and belief, the Plaintiff's and the Tennessee Subclass members' content and information was integral to the services Facebook offered third party app developers like Cambridge Analytica; third party app developers would not have purchased services from Facebook (including advertisements) without access to this information. Indeed, the value of the services Facebook offered to third party app developers was derived from this information.

941. Prior to using the Plaintiff's and the Tennessee Subclass members' content and information, the Defendant never obtained consent.

942. Defendant profited from the commercial use of the Plaintiff's and the Tennessee Subclass members' likeness.

943. Plaintiff and the Tennessee Subclass members did not receive any compensation in return for this use.

944. According to T. C. A. § 47-25-1105, Plaintiff and the Tennessee Subclass members seek the greater of \$5,000 per incident or the actual damages suffered, plus any profits attributable to Defendants' use of the unauthorized use not calculated in actual damages. Plaintiff and the Tennessee Subclass members also reserve the right to punitive damages, costs, reasonable attorney's fees, and injunctive relief as allowed under this statute.

**Claim XLIII. Violations of Virginia Unauthorized Use Statute,  
Va. Code § 8.01-40  
(Against Prioritized Defendant Facebook Inc.)**

945. The Virginia Plaintiff identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Virginia Subclass, incorporates by reference all allegations of this complaint as though fully set forth herein.

946. Va. Code § 8.01-40 prohibits the use of a person's name, portrait or picture for commercial purposes without first obtaining that person's consent, or where appropriate the consent of that person's parent or legal guardian.

947. Defendant Facebook violated this section by allowing access to Plaintiff's and Virginia Subclass members' content and information—including names, like history, photographs, and video—as a service to third parties. On information and belief, the Plaintiff's and Virginia Subclass members' content and information was integral to the services Facebook offered third party app developers like Cambridge Analytica; third party app developers would not have purchased services from Facebook (including advertisements) without access to this information. Indeed, the value of the services Facebook offered to third party app developers was derived from this information.

948. Prior to using the Plaintiff's and Virginia Subclass members' content and information, the Defendant never obtained consent.

949. Defendant profited from the commercial use of the Plaintiff's and Virginia Subclass members' likeness.

950. Plaintiff and Virginia Subclass members did not receive any compensation in return for this use.

951. According to Va. Code § 8.01-40, Plaintiff and Virginia Subclass members seek actual damages suffered, plus any profits attributable to Defendants' use of the unauthorized use not calculated in actual damages. Plaintiff and Virginia Subclass members also reserve the right to punitive damages, costs, and reasonable attorney's fees as allowed under this statute.

**Claim XLIV. Violations of Washington Personality Right Statue,  
Wash. Code § 63.60.050  
(Against Prioritized Defendant Facebook Inc.)**

952. The Washington Plaintiffs identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Washington Subclass, incorporates by reference all allegations of this complaint as though fully set forth herein.

953. Wash. Code § 63.60.050 prohibits the use of a person's name, voice, signature, photograph, or likeness on or in goods, merchandise, or products entered into commerce in that state without first obtaining that person's consent, or where appropriate the consent of that person's parent or legal guardian.

954. Defendant Facebook violated this section by allowing access to Plaintiff's and Washington Subclass members' content and information—including names, like history, photographs, and video—as a service to third parties. On information and belief, Plaintiff's and Washington Subclass members' content and information was integral to the services Facebook offered third party app developers like Cambridge Analytica; third party app developers would not have purchased services from Facebook (including advertisements) without access to this information. Indeed, the value of the services Facebook offered to third party app developers was derived from this information.

955. Prior to using the Plaintiff's and Washington Subclass members' content and information, the Defendant never obtained consent.

956. Defendant profited from the commercial use of the Plaintiff's and Washington Subclass members' likeness.

957. Plaintiff and Washington Subclass members did not receive any compensation in return for this use.

958. According to Wash. Code § 63.60.060 Plaintiff and Washington Subclass members seek the greater of \$1,500 per incident or the actual damages suffered, plus any profits attributable to Defendants' use of the unauthorized use not calculated in actual damages. Plaintiff and Washington Subclass members also reserve the right to costs, and reasonable attorney's fees as allowed under this statute.

**Claim XLV. Violations of Wisconsin Right of Publicity Statute,  
Wis. Stat. § 995.50  
(Against Prioritized Defendant Facebook Inc.)**

959. The Wisconsin Plaintiff identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Wisconsin Subclass, incorporates by reference all allegations of this complaint as though fully set forth herein.

960. Wis. Stat. § 995.50(b) prohibits the use of a name, portrait or picture for the purposes of trade or advertising without first obtaining that person's consent, or where appropriate the consent of that person's parent or legal guardian.

961. Defendant Facebook violated this section by allowing access to Plaintiff's and Wisconsin Subclass members' content and information—including names, like history, photographs, and video—as a service to third parties. On information and belief, Plaintiff's and Wisconsin Subclass members' content and information was integral to the services Facebook offered third party app developers like Cambridge Analytica; third party app developers would not have purchased services from Facebook (including advertisements) without access to this information. Indeed, the value of the services Facebook offered to third party app developers was derived from this information.

962. Prior to using the Plaintiff's and Wisconsin Subclass members' content and information, the Defendant never obtained consent.

963. Defendant profited from the commercial use of the Plaintiff's and Wisconsin Subclass members' likeness.

964. Plaintiff and Wisconsin Subclass members did not receive any compensation in return for this use.

965. According to Wis. Stat. § 995.50, Plaintiff and Wisconsin Subclass members seek actual damages, plus any profits attributable to Defendants' use of the unauthorized use not calculated in actual damages. Plaintiff and Wisconsin Subclass members also reserve the right to costs, reasonable attorney's fees, and injunctive relief as allowed under this statute.

**Claim XLVI. Violations of California Right of Publicity Statute,  
Cal. Civil Code § 3344  
(Against Prioritized Defendant Facebook, and Doe Defendants; Against Non-Prioritized  
Defendants Zuckerberg, Mercer, Bannon and Kogan)  
On Behalf of All Plaintiffs and Classes**

966. Plaintiffs incorporate by reference all allegations of this complaint as though fully set forth herein.

967. California Civil Code § 3344 prohibits the knowing use of a person's name, voice, signature, photograph, or likeness for a commercial gain without first obtaining that person's consent, or where appropriate the consent of that person's parent or legal guardian.

968. Defendants violated this section by allowing access to Plaintiffs' and Class Members' content and information—including names, like history, photographs, and video—as a service to third parties. On information and belief, the content and information of Plaintiffs and Class Members was integral to the services Facebook offered app developers like Cambridge Analytica. App developers would not have purchased services from Facebook (including advertisements) without access to this content and information. Indeed, the value of the services Facebook offered to app developers was derived from this content and information. Thus, Facebook directly benefited from this use of Plaintiffs' content and information.

969. Facebooks' API feeds are "products" for purposes of Civil Code Section 3344.

Additionally, Facebook used its API feeds to advertise for services Facebook offered, such as advertisements. Facebook effectively used access to API feeds containing photographs and likenesses of Plaintiffs and Class Members to sell its advertising services.

970. The photographs and likenesses exploited by Facebook through API feeds includes photographs and videos. Facebook offered these photographs and likenesses to third party app developers and other business partners as part of the API service without regard to Plaintiffs' and Class Members' privacy settings attached to the photographs and videos. Facebook received substantial revenue from publishing this content and information through its API feed in the form of advertising revenue. Facebook linked the payment of advertisements with the continued access to API feeds that included photographs and likenesses of Plaintiffs and Class Members.

971. Prior to using the Plaintiffs' content and information, the Facebook never obtained consent from the Plaintiffs.

972. Plaintiffs received no compensation for the use of their likeness.

973. Facebook had knowledge of the unauthorized uses of Plaintiffs' and Class Members' names, photographs, and likenesses.

974. Plaintiffs were harmed by Facebook's improper use.

975. According to California Civil Code § 3344(a), Plaintiffs seek the greater of \$750 per incident or the actual damages suffered, plus any profits attributable to Facebook's use of the unauthorized use not calculated in actual damages. Plaintiffs also reserve the right to punitive damages, costs, and reasonable attorney's fees as allowed under this statute.

**Claim XLVII. Violations of the Fair Credit Reporting Act**  
**15 U.S.C. §§ 1681 *et seq.***  
**(Against Prioritized Defendant Facebook,,)**  
**On Behalf of All Plaintiffs and Classes**

976. Plaintiffs incorporate by reference all allegations of this complaint as though fully set forth herein.

977. As individuals, Plaintiffs and Class members are consumers entitled to the protections of the FCRA. 15 U.S.C. § 1681a(c).



978. Facebook is a “person” as defined by 15 U.S.C. § 1681a(b).

979. Facebook is a CRA—a “consumer reporting agency” as defined in 15 U.S.C. §§ 1681a(f) which is defined as “any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties . . . .” 15 U.S.C. § 1681a(f).

980. The compromised data was a “consumer report” under the FCRA as defined under 15 U.S.C. § 1681a(d)(1).

981. As a consumer reporting agency, Facebook may only furnish a consumer report under the limited circumstances set forth in 15 U.S.C. § 1681b, “and no other.” 15 U.S.C. § 1681b(a). None of the purposes listed under 15 U.S.C. § 1681b permit credit reporting agencies to furnish consumer reports to unauthorized or unknown entities.

982. Facebook willfully and/or recklessly violated § 1681b and § 1681e(a) by providing impermissible access to consumer reports and by failing to maintain reasonable procedures designed to limit the furnishing of consumer reports to the purposes outlined under section 1681b of the FCRA.

983. As a CRA, Facebook is required to make clear, accurate, and complete disclosures as set forth in 15 U.S.C. 1681g.

984. Facebook failed to make clear, accurate, and complete disclosures, violating 15 U.S.C. § 1681g.

985. As a result of each and every willful violation of FCRA, Plaintiffs and Class members are entitled to: actual damages, pursuant to 15 U.S.C. § 1681n(a)(1); statutory damages, pursuant to 15 U.S.C. § 1681n(a)(1); punitive damages, as this Court may allow, pursuant to 15 U.S.C. § 1681n(a)(2); and reasonable attorneys’ fees and costs pursuant to 15 U.S.C. § 1681n(a)(3).

986. As a result of each and every negligent non-compliance of the FCRA, Plaintiffs and Class members are also entitled to actual damages, pursuant to 15 U.S.C. § 1681o(a)(1); and

reasonable attorney's fees and costs pursuant to 15 U.S.C. § 1681o(a)(2) from Defendant.

**Claim XLVIII. Unlawful Interception of Communications,  
11 Del. Code § 2401  
(Against Prioritized Defendant Facebook, Inc.)**

987. Plaintiffs adopt and incorporate all the allegations of this complaint as if stated fully herein.

988. By reason of the conduct alleged herein, Defendants violated Delaware's Criminal Code protecting persons from electronic surveillance and unlawful interception of communications.

989. According to Chapter 24 of the Title 11 of the Delaware Criminal Code, "Electronic communication" includes "any transfer of signs, signals, writing, images, sounds, data or intelligence of any electromagnetic, photoelectronic or photooptical system." 11 Del. Code § 2401.

990. The messages, posts, images and countless other forms of communication on Facebook user's profiles are considered electronic communications.

991. The statute defines "Electronic communication system" as "any wire, oral, electromagnetic, photooptical, or photoelectronic facilities for the transmission of wire, oral or electronic communications and any computer facilities or related electronic equipment." *Id.*

992. The servers Facebook uses to provide its electronic communication service which facilitate user communication are considered an "electronic communication system".

993. Delaware prohibits the intentional interception of any wire, oral or electronic communication unless party to the communication or with prior consent by one of the parties to the communication. 11 Del. Code § 2402(a).

994. Delaware also prohibits a person or entity providing an electronic communications service to the public from knowingly divulging to any other person or entity the contents of a communication while the communication is in electronic storage by that service. 11 Del. Code § 2422.

995. Facebook, a "person" and "electronic communication service" pursuant to

Delaware Criminal Code, unlawfully and intentionally divulged the contents of Plaintiffs' and Class members' communications.

996. Facebook intentionally divulged the contents of Plaintiffs' and Class members' stored electronic communications by allowing Cambridge Analytica access to their electronic communications which also contained sensitive personal information and identifiers putting Plaintiffs and Class members at risk of being harmed.

997. Section 2409 of the Delaware Criminal Code authorizes a private right of action for actual damages, punitive damages and reasonable attorneys' fees and other litigation costs reasonably incurred to any person whose wire, oral or electronic communication is intercepted, disclosed or used in violation of this code.

998. Plaintiffs and Class members have been harmed by Defendants' misconduct and are entitled to actual damages, punitive damages and reasonable attorneys' fees and costs.

**Claim XLIX. Violation of New Jersey Consumer Fraud Act,  
N.J. Stat. Ann. §§ 56:8-1 et seq.  
(Against Facebook)**

999. Plaintiffs incorporate by reference the allegations in the preceding paragraphs as if fully set forth herein.

1000. Defendants and the New Jersey State Class members are "persons" within the meaning of N.J. STAT. ANN. § 56:8-1(d). Facebook engaged in "sales" of "merchandise" within the meaning of N.J. STAT. ANN. § 56:8-1(c), (d).

1001. The New Jersey Consumer Fraud Act ("New Jersey CFA") makes unlawful "[t]he act, use or employment by any person of any unconscionable commercial practice, deception, fraud, false pretense, false promise, misrepresentation, or the knowing concealment, suppression or omission of any material fact with the intent that others rely upon such concealment, suppression or omission, in connection with the sale or advertisement of any merchandise or real estate, or with the subsequent performance of such person as aforesaid, whether or not any person has in fact been misled, deceived or damaged thereby..." N.J. STAT. ANN. § 56:8-2.

1002. As set forth above, Facebook, while operating in New Jersey, engaged, in

unconscionable commercial practices, deception, misrepresentation, and the knowing concealment, suppression, and omission of material facts with intent that others rely on such concealment, suppression, and omission, in connection with the sale and advertisement of services, in violation of N.J. Stat. Ann. § 56:8-2. This includes:

- A. Collecting, storing, and using vast quantities of highly sensitive personal information and which Facebook failed to adequately protect from unauthorized and/or criminal access;
- B. Failing to employ technology and systems to promptly detect unauthorized access to the personal information with which they were entrusted;
- C. Unreasonably delaying giving notice to consumers after it became aware of unauthorized access to the personal information;
- D. Knowingly and fraudulently failing to provide accurate, timely information to consumers about the extent to which their personal information had been compromised; and
- E. Making false and deceptive representations and communications concerning the purpose of and reasons for collecting highly sensitive personal information.

1003. Facebook's breach of its duties has directly and proximately caused Plaintiffs and the New Jersey Subclass to suffer an ascertainable loss of money and property, including the loss of their personal information and foreseeably causing them to expend time and resources investigating the extent to which their personal information has been compromised.

1004. The above unlawful and deceptive acts and practices and acts by Facebook were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiffs and the New Jersey Subclass that they could not reasonably avoid. This substantial injury outweighed any benefits to consumers or to competition.

1005. Plaintiffs and the New Jersey Subclass seek relief under N.J. Stat. Ann. § 56:8-19, including, but not limited to, injunctive relief, other equitable actual damages (to be proven at

trial), disgorgement of wrongfully obtained profits, treble damages, and attorneys' fees and costs.

**Claim L. Intentional Misrepresentation  
(Against Facebook)  
On Behalf of All Plaintiffs and Classes**

1006. Plaintiffs reallege and incorporate by reference all allegations of this complaint as though fully set forth herein.

1007. Facebook intentionally misrepresented the use and access to the data that Plaintiffs and Class Members owned on their Facebook sites. Defendant Facebook intentionally misrepresented that it would not disclose Plaintiffs' and the Class Members' Personal Information without authorization.

1008. Facebook intentionally misrepresented to the Plaintiffs and the Class the protection and privacy of their Facebook data as described above, and in other means. In addition, Facebook intentionally failed to disclose that information was available to device manufacturers.

1009. Defendant's representations were false because Facebook knowingly and intentionally provided the Personal Information of Plaintiffs and Class Members to device manufacturers, and did so for Facebook's financial and commercial advantage without either permission or sufficient consent from Plaintiffs and Class Members.

1010. Facebook's representations were material to Plaintiffs' and Class Members' decision to post and provide Personal Information on Facebook.

1011. Plaintiffs and the Class Members justifiably relied on the representations Facebook made in its Privacy Policy and elsewhere on their website and acted in reliance on those representations by placing Personal Information on Facebook.

1012. Facebook knew of the falsity of its representations, and its representations were made to deceive Plaintiffs and Class Members into providing Personal Information that could be used for Facebook's financial and marketing advantage.

1013. Facebook knew it did not have permission to allow device manufacturers to collect and/or access Personal Information because it did not attempt to obtain permission from

Plaintiffs and the Class Members.

1014. Plaintiffs and the Class Members suffered injury-in-fact and lost property as a proximate result of Facebook's intentional misrepresentation.

1015. As a direct and proximate result of Facebook's intentional misrepresentation, Plaintiffs and Class Members suffered injuries, damages, losses or harm, including but not limited to annoyance, interference, concern, lost time, the loss of personal property, and the need for the cost of effective credit and privacy security, justifying an award of compensatory and punitive damages.

#### **X. PRAYER FOR RELIEF**

1016. Plaintiffs, individually and on behalf of Class Members, request that the Court enter judgment in their favor and against Defendants, as follows:

1017. Certify the Classes and appoint Plaintiffs as Class Representatives;

1018. Enter Judgment against Defendants on Plaintiffs' and Class Members' asserted causes of action;

1019. Award Plaintiffs and Class Members appropriate relief, including actual and statutory damages, restitution, disgorgement, and punitive damages;

1020. Award equitable, injunctive, and declaratory relief as may be appropriate;

1021. Award all costs, including experts' fees and attorneys' fees, as well as the costs of prosecuting this action;

1022. Award pre-judgment and post-judgment interest as prescribed by law; and

1023. Grant additional legal and equitable relief as this Court may find just and proper.

#### **XI. DEMAND FOR JURY TRIAL**

1024. Plaintiffs, on behalf of themselves and all others similarly situated, hereby demand a trial by jury on all the issues so triable.

Dated: September 21, 2018

KELLER ROHRBACK L.L.P.

By: /s/ Derek W. Loeser  
Derek W. Loeser

Derek W. Loeser (admitted *pro hac vice*)  
Lynn Lincoln Sarko (admitted *pro hac vice*)  
Gretchen Freeman Cappio (admitted *pro hac vice*)  
Cari Campen Laufenberg (admitted *pro hac vice*)  
1201 Third Avenue, Suite 3200  
Seattle, WA 98101  
Tel.: (206) 623-1900  
Fax: (206) 623-3384  
dloeser@kellerrohrback.com  
lsarko@kellerrohrback.com  
gcappio@kellerrohrback.com  
claufenberg@kellerrohrback.com

Christopher Springer (SBN 291180)  
801 Garden Street, Suite 301  
Santa Barbara, CA 93101  
Tel.: (805) 456-1496  
Fax: (805) 456-1497  
cspringer@kellerrohrback.com

BLEICHMAR FONTI & AULD LLP

Lesley E. Weaver (SBN 191305)  
Matthew S. Weiler (SBN 236052)  
Emily C. Aldridge (SBN 299236)  
555 12th Street, Suite 1600  
Oakland, CA 94607  
Tel.: (415) 445-4003  
Fax: (415) 445-4020  
lweaver@bfalaw.com  
mweiler@bfalaw.com  
ealdridge@bfalaw.com

*Plaintiffs' Co-Lead Counsel*